MANUAL

Versão: 30/09/2014

Versão: 08/06/2013

AKER Web Defender

AKER

www.aker.com.br

Índice

ÍNDICE 2

ÍNDICE DE IMAGENS 4

1. INTRODUÇÃO 7

1.1. COMO ESTÁ DISPOSTO ESTE MANUAL 7
1.2. O QUE É UM WAF? 7

2. AKER WEB DEFENDER 14

2.1. EXEMPLO DE TOPOLOGIA DO AKER WEB DEFENDER 15
2.2. PRINCIPAIS CARACTERÍSTICAS DO AKER WEB DEFENDER 18
2.3. CLASSES DE ATAQUES: 19
PRÉ REQUISITOS 20
2.4. ACESSANDO O AKER WEB DEFENDER –BOX 20
2.5. ACESSANDO O AKER WEB DEFENDER – VM 21
2.6. SESSÃO 29
2.7. PAINEL DE CONTROLE 30

3. MENUS 33

3.1. LICENÇA 33
3.2. INCIDENTES 34
- FILTROS 35
3.3. RELATÓRIOS 38
3.4. ALTERAR SENHA 38
3.5. DESLIGAR 39
3.6. SAIR 39

4. MÓDULO CONFIGURAÇÕES 41

4.1. WEB APPLICATION FIREWALL 41
4.2. SERVIDORES REAIS 42
4.2.1 Incluindo um novo Servidor Real 42
4.2.2 Incluindo o IP do Servidor Real 43
4.2.3 Incluindo a porta do Servidor Real 43
4.3. VIRTUAL HOSTS 44
4.3.1 Incluindo um novo Sitio Virtual (Virtual Host) 44
4.3.2 Configurando Portas e Aliases para o novo Sitio Virtual 45
4.4. ASSINATURAS 47
4.5. APRENDIZADO 51
4.6. POSITIVO 52
4.7. INTELIGÊNCIA ARTIFICIAL 54
4.8. SISTEMA 55
4.9. INTERFACES 56
4.9.1 DNS: 57
4.9.2 NTP: 58
4.9.3 ROTAS: 59
4.9.4 HTTP Tunning 60
4.10. FERRAMENTAS 60
4.10.1 Usuários 61
4.10.2 Log 62

4.10.3 Backup 63
4.10.4 Restore 63
4.11. CONFIGURAÇÕES 64
5. F.A.Q. 68

Índice de imagens

Figura 1 - Crescimento do uso de aplicações web 8
Figura 2 - Camadas do perímetro de segurança 10
Figura 3 - Topologia de rede com um WAF 10
Figura 4 - Topologia de rede sem um WAF 11
Figura 5 - Lista de ameaças 11
Figura 6 - Ameaças que o Aker Web Defender pode detectar 12
Figura 7 - Comparativo do Aker Web Defender com outros softwares 12
Figura 8 - Modelo de Topologia com 2 interfaces 16
Figura 9 - Modelo de Topologia com 2 interfaces com o Aker Web Defender 16
Figura 10 - Modelo de Topologia com até 7 interfaces 17
Figura 11 - Modelo de Topologia com até 7 interfaces com o Aker Web Defender 18
Figura 12 - Tela de acesso do Aker Web Defender 29
Figura 13 - Painel de controle 31
Figura 14 - Menus 33
Figura 15 - Licença 34
Figura 16 - Aba incidentes 35
Figura 17 - Filtragem de Incidentes 35
Figura 18 - Módulo “Relatórios” 38
Figura 19 - Módulo “Alterar Senha” 38
Figura 20 - Menu de Opções do Aker Web Defender 39
Figura 21 - Módulo Configurações 41
Figura 22 - Web Application Firewall 41
Figura 23 - Aba Servidores Reais 42
Figura 24 - Servidor Real 43
Figura 25 - Incluindo o IP do Servidor Real 43
Figura 26 - Incluindo a porta do Servidor Real 44
Figura 27 - Sítios Virtuais 44
Figura 28 - Incluindo Sítios Virtuais 45
Figura 29 - Aba Aliases e Portas 46
Figura 30 - Aba Porta 46
Figura 31 - Aba Aliases 47
Figura 32 - Definindo Apelido 47
Figura 33 - Assinaturas 48
Figura 34 - Assinaturas (conexão) 48
Figura 35 - Assinaturas (Headers) 49
Figura 36 - Assinaturas (RequestBody) 50
Figura 37 - Assinaturas (ResponseBody) 50
Figura 38 - Inserindo Assinatura na Whitelist 51
Figura 39 – Aprendizado 51
Figura 40 - Configurando o módulo Aprendizado 51
Figura 41 - Positivo 52
Figura 42 - módulo visualização 53
Figura 43 – Configurando do positivo de visualização 53
Figura 44 - Inteligência Artificial 54
Figura 45 - Detector XSRF 54
Figura 46 - Opções de ataques 55

Figura 47 - Detector crawling 55
Figura 48 - Sistema 56
Figura 49 - Interfaces 56
Figura 50 - Aba DNS 58
Figura 51 - Aba NTP 58
Figura 52 - Aba Rotas 59
Figura 53 - HTTP Tunning 60
Figura 54 - Ferramentas 60
Figura 55 - Aba Usuários 61
Figura 56 - Janela de inclusão de usuário 61
Figura 57 - Aba Atualizações 62
Figura 58 - Detalhamento do log 62
Figura 59 - Aba Backup 63
Figura 60 - Aba Restore 63
Figura 61 - Configurações 64
Figura 62 - Modo Janelas 64
Figura 63 - Modo abas 65
Figura 64 - Confirmação para executar ação 65

Introdução

1. Introdução

*Seja bem-vindo ao manual do usuário do **Aker Web Defender**.*

Nos próximos capítulos você aprenderá como configurar esta poderosa ferramenta de proteção aos dados e a integridade de sua empresa. Esta introdução tem como objetivo descrever a organização deste manual tornando sua leitura a mais simples e agradável possível.

1.1. Como está disposto este manual

Este manual é organizado em vários capítulos. Cada capítulo mostra um aspecto da configuração do produto e todas as informações relevantes ao aspecto tratado.

Todos os capítulos começam com uma introdução teórica sobre o tema a ser tratado seguido dos aspectos específicos de configuração do **Aker Web Defender**. Juntamente com esta introdução teórica, alguns módulos possuem exemplos práticos do uso do serviço a ser configurado, em situações hipotéticas, porém, bastante próximas da realidade. Buscamos com isso tornar o entendimento das diversas variáveis de configuração o mais simples possível.

Recomendamos que este manual seja lido, pelo menos uma vez por inteiro, na ordem apresentada. Posteriormente, se for necessário, pode-se usá-lo como fonte de referência.

Para facilitar seu uso como referência, os capítulos estão divididos em tópicos, com acesso imediato pelo índice principal. Desta forma, pode-se achar facilmente a informação desejada.

No decorrer deste manual, aparecerá o símbolo ( ) seguido de uma frase escrita em letras vermelhas. Isto significa que a frase em questão é uma observação muito importante e deve ser totalmente entendida antes que se prossiga com a leitura do capítulo.

1.2. O que é um WAF?

O WAF (Firewall para aplicações WEB) oferece proteção específica contra ataques às aplicações Web. Diferente dos IPS (Sistema de prevenção de intrusos), o WAF só entende e trabalha na camada de aplicação. Ele é especialista em análises de tráfego HTTP, e inspeciona tráfego HTTPS (ssl), além de trabalhar com análises de assinaturas e análises comportamentais, utilizando o modo positivo. E ainda possui recursos de inteligência artificial.

Qual a importância das aplicações Web nas empresas:

- Economia de tempo
- Compatibilidade
- Baixo consumo de recursos
- Acesso imediato
- Usuários trabalhando simultaneamente
- Alta disponibilidade
- Outros

Com a grande importância das aplicações Web nas empresas, a crescimento do uso de aplicações web no mercado não tem limite, mas juntamente com esse crescimento novos problemas aparecem, pois as aplicações web se tornaram o principal alvo de atacantes. Segundo o ***Gartner***, 75 % dos ataques cibernéticos estão direcionados às aplicações Web.

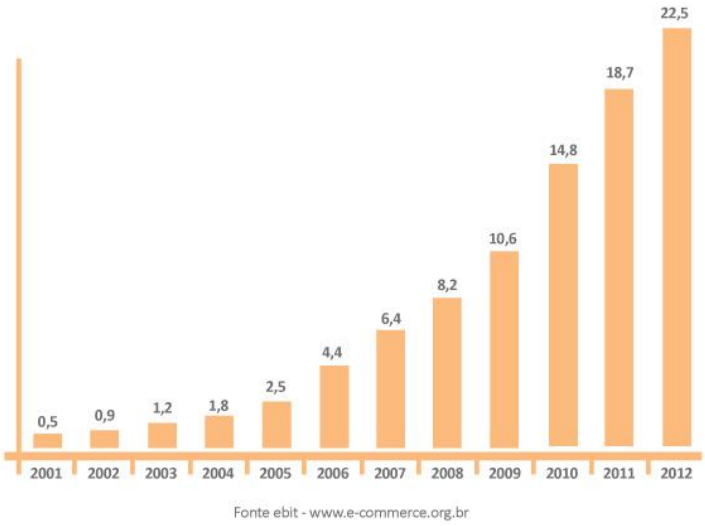


Figura 1 - Crescimento do uso de aplicações web

Exemplos de Aplicações Web:

- Blog;
- Portais de negócios;
- Webmail (Gmail, Hotmail, etc.,);

Por que existem tantos problemas de segurança nas aplicações Web?

- Falta de cultura em programação segura;
- Falta de um ciclo de programação segura dentro das empresas;
- Falta de política de retenção de programadores nas empresas;
- Terceirização do desenvolvimento das aplicações;
- Programadores preocupados com funcionalidades, e não com segurança;
- Legado de aplicações;

Por que as aplicações Web são o foco dos ataques cibernéticos?

- Porque as aplicações conversam diretamente com os bancos de dados das empresas;
- Os atacantes sabem que as empresas não possuem um ciclo de desenvolvimento seguro;
- Por que, em nível de infraestrutura de rede, os atacantes sabem que as aplicações não podem ser protegidas por firewalls convencionais e que os IPSs não são capazes de deter os ataques na camada de aplicação;

Qual a diferença entre um Hacker e um Cracker?

Os dois termos referem-se à indivíduos que são experts em computadores, que possuem habilidades extraordinárias ao lidar com sistemas e programação, sendo que:

Hackers são profissionais que trabalham através de diversas técnicas e inteligentes com o intuito de melhor a segurança e funcionalidade e softwares.

Crackers são indivíduos que possuem o mesmo conhecimento que Hackers, mas usa seu conhecimento para invadir computadores, sistemas, redes etc., para roubar informações confidencias que na maioria das vezes são vendidas ou utilizadas para aplicar golpes na internet.

O que motiva um atacante (cracker)?

Antigamente os atacantes eram motivados por fama e o prestígio frente à comunidade de Crackers. Nos dias atuais eles são motivados por prestígio, ganhos financeiros por meio de golpes, e também para protestar (Anonymous).

Uma das principais técnicas de ataque usadas pelos Crackers é o SQL Injection:

O SQL Injection ocorre quando é possível injetar códigos SQL em uma aplicação, utilizando parâmetros de entrada que são posteriormente repassados ao banco de dados para execução. Estas ações executadas ocorrem com o mesmo nível de privilégio do usuário que está sendo utilizado para se conectar ao banco de dados. Esta vulnerabilidade já possui mais de 15 anos e ainda continua sendo a forma mais utilizada por Crackers devido à falta de segurança nas empresas.

Entendendo o perímetro.

Um perímetro de segurança é dividido em 3 camadas:

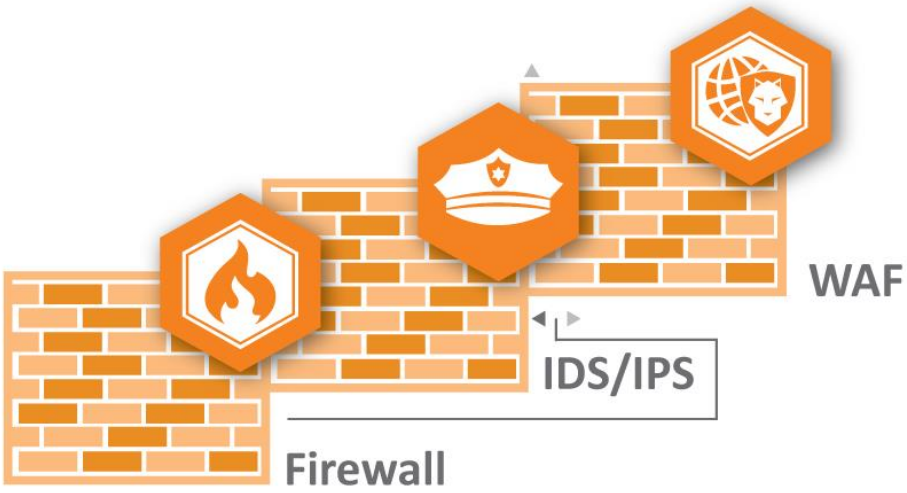


Figura 2 - Camadas do perímetro de segurança

1. **Firewall**: inspeciona IP e portas, normalmente não supervisionam tráfego HTTP/S de forma adequada;
2. **IPS/IDS**: Assinaturas conhecidas, sendo possível, evadir assinaturas, não inspecionar o Tráfego SSl, não entende com perfeição o HTTP, nem as particularidades das aplicações gerando um alto número de falsos positivos, e não consegue fazer controle de aplicações. Além de ter o foco principal em assinaturas e não na aplicação, não conseguem proteger ataques "zero day", não é possível "normalizar" o tráfego para detectar ataques ofuscados, se esquece do tráfego criptografado;
3. **WAF**: pode detectar e bloquear ataques às aplicações web, oferecendo mais controle na estrutura do aplicativo (URLs, cookies, cabeçalhos, formulários de sessão, ações SOAP, elementos XML, etc.);

Topologia de rede com um WAF:

Figura 3 - Topologia de rede com um WAF

Topologia de rede sem um WAF:

Figura 4 - Topologia de rede sem um WAF

A seguir a lista de ameaças que Firewalls e IPSs conseguem detectar:

Ameaça	Firewalls/IPS
Cookie poisoning	Assinaturas
Hidden field manipulation	Assinaturas
Cross Site scripting	Assinaturas
Ataques de injeção	⊘
Comandos Stealth	⊘
Parameter Tampering	⊘
Buffer overflow	⊘
Google Hacks	⊘
Forceful Browsing	⊘
Roubo de Identidade	⊘
DoS de Aplicação	⊘
Roubo de Dados	⊘

Figura 5 - Lista de ameaças

A seguir ameaças que o Aker Web Defender pode detectar:

Problema	Protege	Não Protege
Violações de protocolo HTTP	✓	
SQL Injection	✓	
LDAP Injection	✓	
Injeção de comandos no sistema operacional	✓	
Cross-Site Scripting (Refletido e Armazenado)	✓	
Cookie Tampering	✓	
Buffer Overflow	✓	
Remote File Include	✓	
Information Leak	✓	
Brute Force Login	✓	
Negação de Serviço	✓*	
Design (Arquitetura)		⊘

Figura 6 - Ameaças que o Aker Web Defender pode detectar

Comparativo do Aker Web Defender com outros softwares do mercado:

Funcionalidade	Imperva SecureSphere	IBM Data Power	TrustWave Webdefend	AKER Web Defender
SSL Termination	✓	✓	✓	✓
HTTP protocol filtering	✓	✓	✓	✓
Protection SQL injection	✓	✓	✓	✓
Virtual Patching	✓	✓	✓	✓
Modo Positivo	✓	✓	✓	✓
HTTP, HTTPS (SSL), XML, Web services, SOAP e AJAX	✓	✓	✓	✓
Sistema especialista para detecção de ataques	⊘	⊘	⊘	✓
Rede bayesiana para detecção de ataques	⊘	⊘	⊘	✓
Rede neural para detecção de ataques	⊘	⊘	⊘	✓

Figura 7 - Comparativo do Aker Web Defender com outros softwares

Aker Web Defender

2. Aker Web Defender

Firewalls convencionais e os Sistemas de prevenção de intrusões (**IPS-Intrusion Prevention System**) não são capazes de detectar e bloquear ataques na camada de aplicação, isso explica por que as aplicações são o alvo preferido dos atacantes.

Baseado nesse fato percebeu-se a necessidade de desenvolver um novo método que pudesse analisar as particularidades da camada de aplicação e que tomasse decisões que pudessem bloquear ataques contra as aplicações.

A ideia do **Aker Web Defender** é analisar o protocolo específico da aplicação e tomar decisões dentro das particularidades de cada aplicação, criando uma complexidade infinitamente maior do que configurar regras de fluxo de tráfego TCP/IP como acontece nos firewalls convencionais.

O **Aker Web Defender** é um appliance desenvolvido com foco em segurança. Seu sistema operacional é configurado de acordo com as melhores práticas para suportar os mais duros ataques. Ele é fornecido em um Appliance robusto, seguro e eficaz, onde software e hardware trabalham em conjunto para atender requisições externas e internas aos servidores Web de sua empresa, configurado o sistema de acordo com as melhores práticas para suportar os mais duros ataques.

Atuando diretamente na camada 7 (aplicação) do modelo OSI como um proxy reverso, o **Aker Web Defender** é capaz de interceptar todas as requisições do cliente e as respostas do servidor Web, sendo capaz de detectar e bloquear ataques em HTTP, HTTPS, SOAP, XML-RPC, Web Service, entre outros.

Alguns firewalls de aplicação adotam o conceito de "***assinaturas de ataques***" com intuito de detectar ataques específicos, enquanto outros adotam o conceito de "***anomalia de comportamento***" com intuito de detectar ataques Por meio de tráfego anormal, o **Aker Web Defender** reúne o melhor dos dois mundos em um único produto.

2.1. Exemplo de Topologia do Aker Web Defender

O Aker Web Defender foi desenvolvido para facilitar a implantação e administração na rede do cliente entre outras vantagens como, por exemplo, o fato que o administrador de rede não precisa criar rotas e administrar diversos fluxos de dados como FTP, SSH, SMTP e outros protocolos através do firewall de aplicação.

A seguir dois exemplos de topologia do Aker Web Defender:

É obrigatório que a Eth0 e a Eth1 façam parte da mesma rede.

Exemplos:
Eth0=192.168.0.3/24 ->eth1=192.168.0.11/24

Eth0=10.10.0.15/24 -> eth1=10.10.0.4/24

A versão SVM do Aker Web Defender suporta até 2 interfaces de rede, já na versão Appliance podemos implementar qualquer uma das duas topologias apresentadas.

- **EXEMPLO 01**

***Modelo de Topologia com 2 interfaces**:*

No primeiro exemplo todos os servidores Web estão na mesma rede, ou seja, o Aker Web Defender será instalado na mesma rede onde se encontram os servidores Web do cliente (*neste modelo de topologia não serão protegidos os servidores que se encontrem em outras redes*).

CASE:
Na DMZ do cliente existe três servidores Web com os endereços *192.168.0.10/24, 192.168.0.11/24 e 192.168.0.12/24* e o gateway da DMZ é o *192.168.0.1/24,* conforme exibido na imagem a seguir:

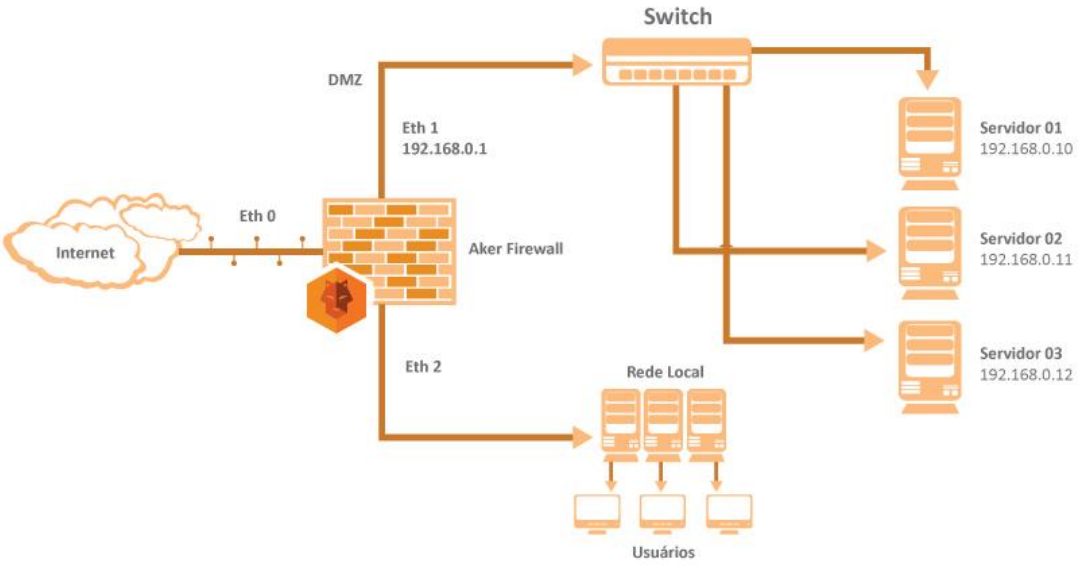


Figura 8 - Modelo de Topologia com 2 interfaces

O Aker Web Defender será instalado na mesma rede utilizando dois endereços IPs do mesmo segmento de rede, neste exemplo a Eth0 do Aker Web Defender terá o IP: *102.168.0.2/24* e a Eth1 terá o IP: *192.168.0.3/24* conforme exibido na imagem a seguir:

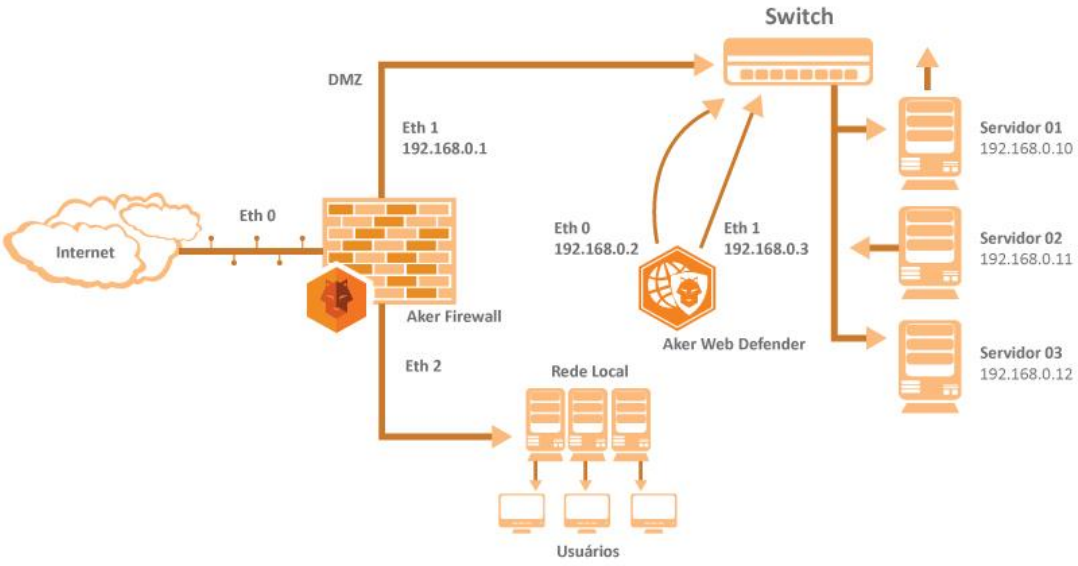


Figura 9 - Modelo de Topologia com 2 interfaces com o Aker Web Defender

Repare que o Aker Web Defender está instalado em paralelo com relação aos servidores Web, isso é muito importante pois permite que o usuário continue gerenciando os serviços de FTP, SSH, TS, SMTP, entre outras coisas. No firewall de borda será deixado apenas a análises de Tráfego HTTP e HTTPS no Aker Web Defender.

Aker Web Defender configura as “Rotas” automaticamente ao cadastrar os IPs de licenciamento e ao criar os “Servidores Reais” que neste caso deverão estar obrigatoriamente na mesma rede.

- **EXEMPLO 02**

Modelo de Topologia com até 7 interfaces:

Neste exemplo a utilização do Appliance e os servidores Web poderão estar em redes diferentes (DMZs).

Case:

Na infraestrutura de redes do cliente existem duas DMZs.

Na DMZ #1 existe três servidores Web com os endereços *192.168.0.10/24, 192.168.0.11/24 e 192.168.0.12/24* e na DMZ #2 existe dois servidores Web com os endereços *10.10.0.15/24 e 10.10.0.16/24* conforme exibido na imagem a seguir:

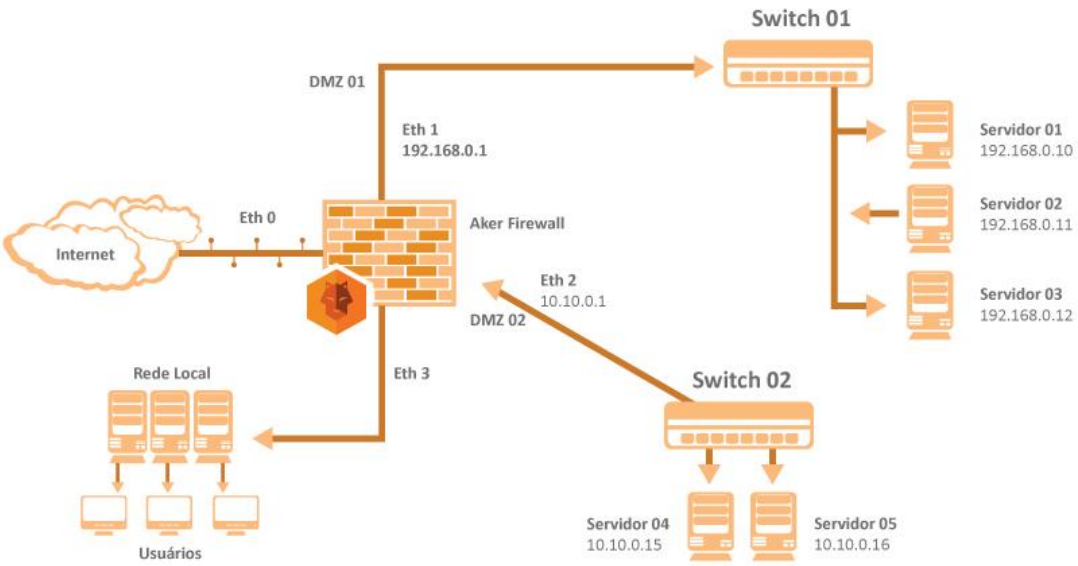


Figura 10 - Modelo de Topologia com até 7 interfaces

O Aker Web Defender será instalado na DMZ #1 utilizando dois endereços IPs do mesmo segmento de rede, neste exemplo a Eth0 do Aker Web Defender terá o IP: *192.168.0.2/24* e a Eth1 terá o IP: *192.168.0.3/24*, para proteger os servidores Web que estão localizados na DMZ #2 serão utilizadas três portas do appliance onde será configurado o IP: *10.10.0.7/24* em seguida é instalado um cabo de rede entre a porta três (eth3) do appliance e uma das portas do Switch da DMZ #2 conforme exibido na imagem a seguir:

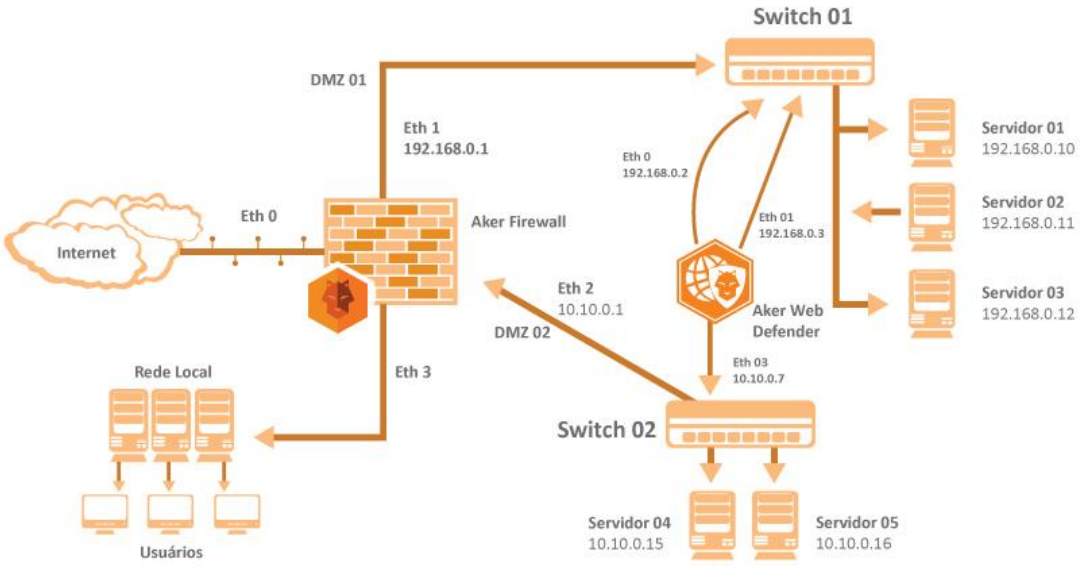


Figura 11 - Modelo de Topologia com até 7 interfaces com o Aker Web Defender

Repare que o Aker Web Defender ficou instalado em paralelo com relação aos servidores Web da DMZ #1, isso é muito importante pois permitirá que o usuário continue fazendo o gerenciamento dos serviços de FTP, SSH, TS, SMTP, entre outas coisa. No firewall de borda será feito apenas a análises de Tráfego HTTP e HTTPS no Aker Web Defender, repare agora que através da eth3=10.10.0.7/24 o Aker Web Defender passou a fazer parte da rede local da DMZ #2.

Em qualquer situação o Tráfego Web deverá ser redirecionado para a Eth0 do Aker Web Defender quem analisará e encaminhará o mesmo para o servidor Web de destino.

2.2. Principais Características do Aker Web Defender

Abaixo seguem as principais características do **Aker Web Defender**:

- Interface de administração em idioma português (Brasil);
- Relatórios de Segurança;
- Capaz de analisar tráfego encriptado (TLS/SSL) trabalhando com certificados digitais,
- Aceita conexão com os sistemas operacionais Linux, Windows 98/200/XP/Vista, Windows 7 e Windows 8;
- Conformidade com o PCI Security Standards Council;
- Proteção contra as vulnerabilidades listadas no OWASP TOP 10;

- Imune a técnicas de evasão utilizando os protocolos IP e TCP;
- Inspeção bidirecional de ataques;
- Constante atualização de assinaturas de ataques;
- Regras de detecção são exaustivamente testadas.

O **Aker Web Defender** visa oferecer para seus clientes os benefícios a seguir:

- Permitir que a empresa, defina o controle de acesso interno/externo;
- Oferecer os mais altos níveis de vigilância das aplicações em tempo real;
- Permitir que a empresa, implemente as mais avançadas soluções de segurança.

2.3. Classes de Ataques:

O Firewall de Aplicação **Aker Web Defender** fornece proteção por default para todos os ataques comuns direcionados à aplicações web, incluindo SQL injection, Cross-Site-Scripting e outros.

Visando oferecer maior segurança para seus clientes, a Aker traz mais um nova poderosa ferramenta para sua proteção, o **Aker Web Defender** que foi projetado para combater por padrão todos os tipos de ataques que foram categorizados como ameaças significativas, incluindo:

1. **Violações do protocolo HTTP;**
2. **SQL Injection;**
3. **LDAP Injection;**
4. **Cookie Tampering;**
5. **Cross-Site Scripting (XSS);**
6. **Buffer Overflow;**
7. **OS Command Execution;**
8. **Remote Code Inclusion;**
9. **Server Side Includes (SSI) Injection;**

10. **File disclosure;**
11. **Information Leak;**
12. **Scanners de vulnerabilidade Web e Crawlers;**
13. **Worms e Web Shell Backdoors;**
14. **Ausência de tratamento de erros do Webserver;**
15. **Bloqueia ataques em HTTP e HTTPS;**
16. **Bloqueia ataques em SOAPe XML-RCP;**
17. **Bloqueia ataques em Web Service entre outros.**

Pré Requisitos

Para criar uma assinatura no **Aker Web Defender**, o usuário deve ter conhecimentos de ***HTTP, Expressões Regulares e Ataques na camada de aplicação***. Abaixo algumas referências:

- *http://pt.wikipedia.org/wiki/HTTP*
- *http://pt.wikipedia.org/wiki/Express%C3%B5es_regulares*
- *https://www.owasp.org/index.php/Main_Page*

2.4. Acessando o Aker Web Defender –Box

Após concluir a instalação do Aker Web Defender se deve acessar o IP: https://192.168.0.100:8051.

Para acessar o Aker Web Defender (Box) siga os passos a seguir:

- Conecte um computador em seu Box do Aker Web Defender usando um cabo de rede, e em seguida configure a interface de rede de seu computador como no exemplo abaixo:

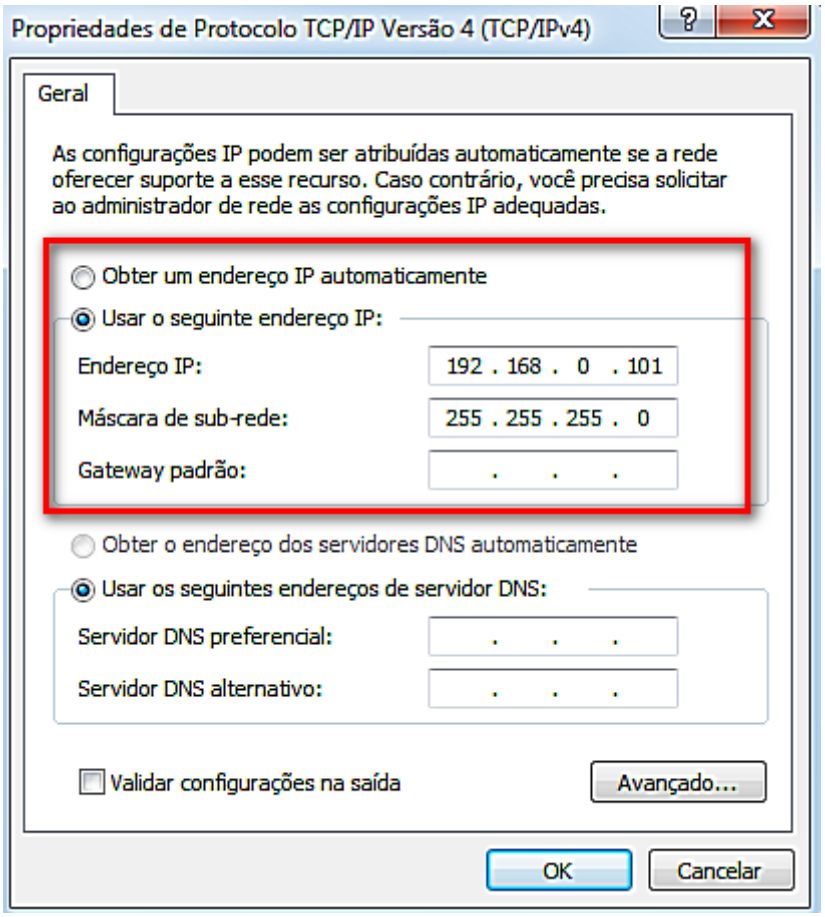

Propriedades de Protocolo TCP/IP Versão 4 (TCP/IPv4)
Geral
As configurações IP podem ser atribuídas automaticamente se a rede oferecer suporte a esse recurso. Caso contrário, você precisa solicitar ao administrador de rede as configurações IP adequadas.
Obter um endereço IP automaticamente
Usar o seguinte endereço IP:
Endereço IP: 192 . 168 . 0 . 101
Máscara de sub-rede: 255 . 255 . 255 . 0
Gateway padrão:
Obter o endereço dos servidores DNS automaticamente
Usar os seguintes endereços de servidor DNS:
Servidor DNS preferencial:
Servidor DNS alternativo:
Validar configurações na saída
Avançado...
OK
Cancelar

Figura 12 - Aker Web Defender Box

Endereço IP: 192.168.0.101

Máscara de sub-rede: 255.255.255.0

Clique em '**ok**'.

Abra o browser, e acesse o endereço: https://192.168.0.100:8051/

2.5. Acessando o Aker Web Defender – VM

Após concluir a instalação do Aker Web Defender se deve acessar o IP: https://192.168.0.100:8051.

O download do Aker Web Defender (VM-ware ESXi5) pode ser feito por meio do link:

http://download.aker.com.br/prod/current/servidor/akerwebdefender-1.0.1-pt-vm-001.zip

Após concluir o download, clique duas vezes no arquivo '***akerwebdefender-1.0.1-pt-vm-001***' para que a importação da maquina virtual seja iniciada.

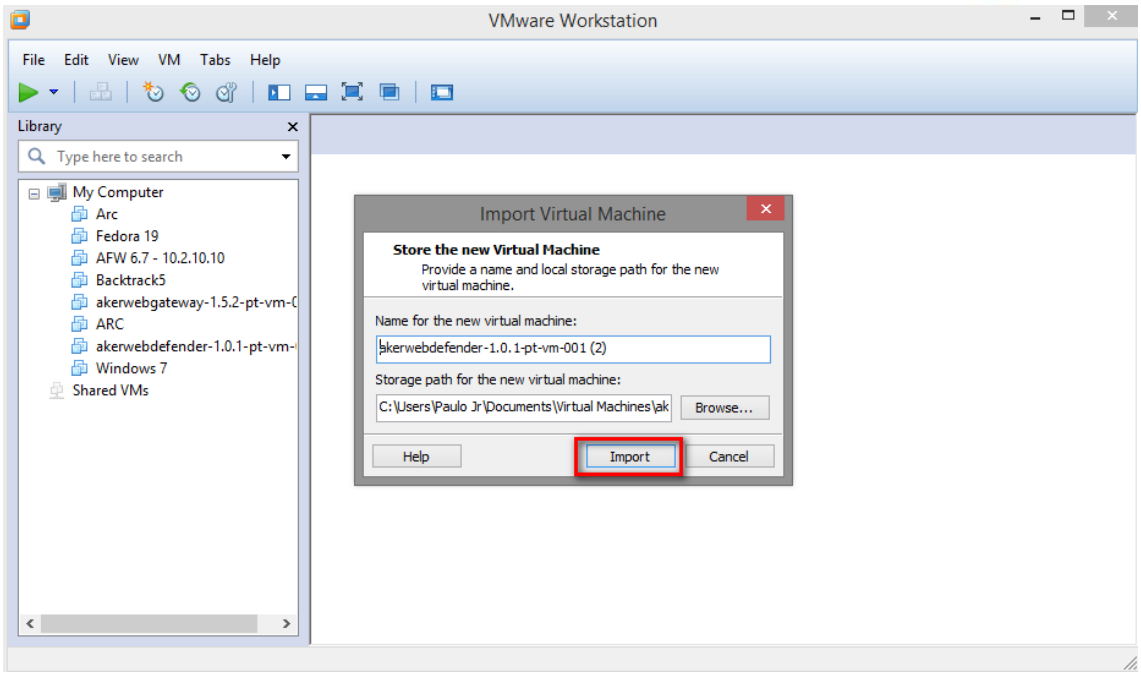
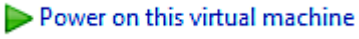


Figura 13 - Importando máquina virtual

Clique em '**Import**', e aguarde até que o processo seja concluído.

Figura 14 - Ligando a máquina virtual

Em seguida, clique em 

.

Ao concluir a inicialização da maquina virtual do Aker Web Defender, se deve configurar a interface de rede de sua maquina para acessar o Aker Web Defender.

Para isso siga os passos a seguir:

Acesse as propriedades de sua interface de rede (o processo exibido a seguir é feito em uma maquina Windows 8). Para isso navegue até o menu iniciar, e abra a '**Central de Rede e Compartilhamento**'.

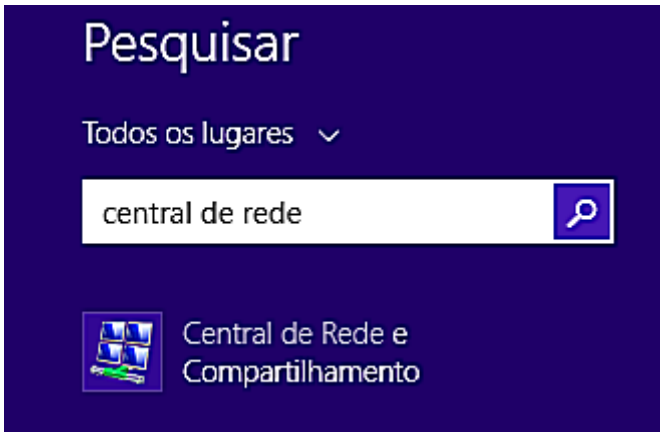


Figura 15 - Central de rede

Em seguida, clique no adaptador de rede em uso.

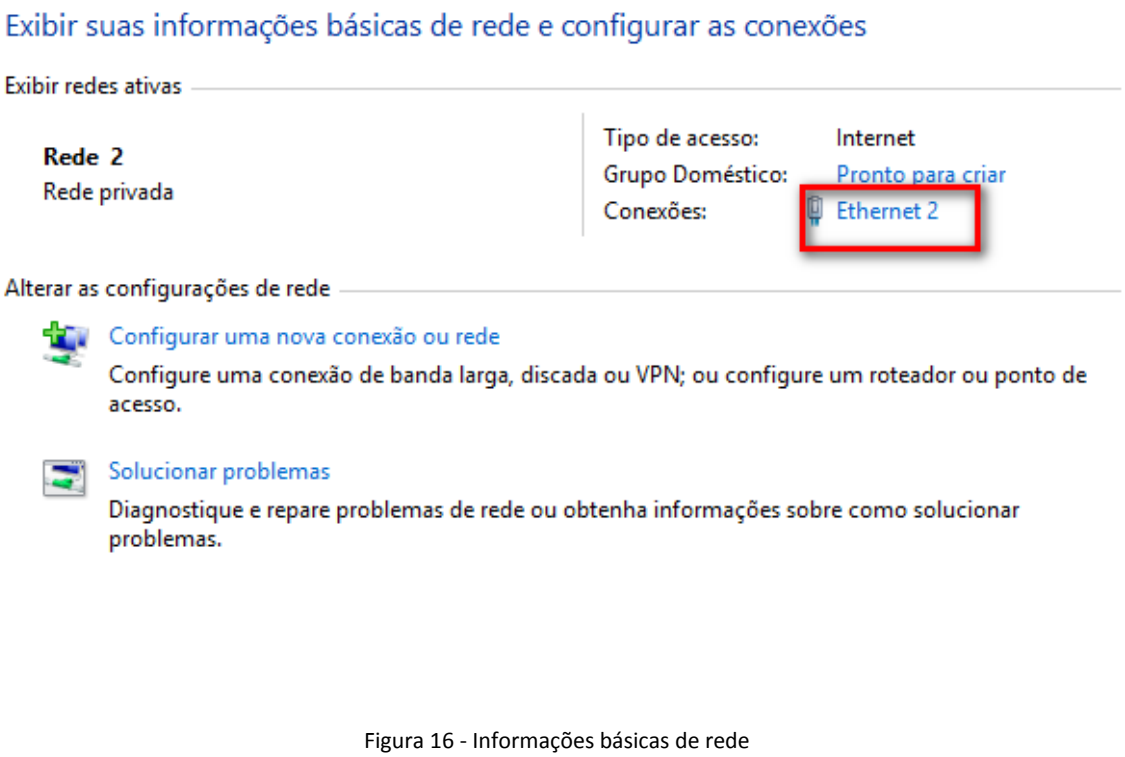

Exibir suas informações básicas de rede e configurar as conexões
Exibir redes ativas
Rede 2
Rede privada
Tipo de acesso: Internet
Grupo Doméstico: Pronto para criar
Conexões: Ethernet 2
Alterar as configurações de rede
Configurar uma nova conexão ou rede
Configure uma conexão de banda larga, discada ou VPN; ou configure um roteador ou ponto de acesso.
Solucionar problemas
Diagnostique e repare problemas de rede ou obtenha informações sobre como solucionar problemas.

Figura 16 - Informações básicas de rede

A janela '**Status de Conexão local'** será exibida, clique em '**Propriedades**'.

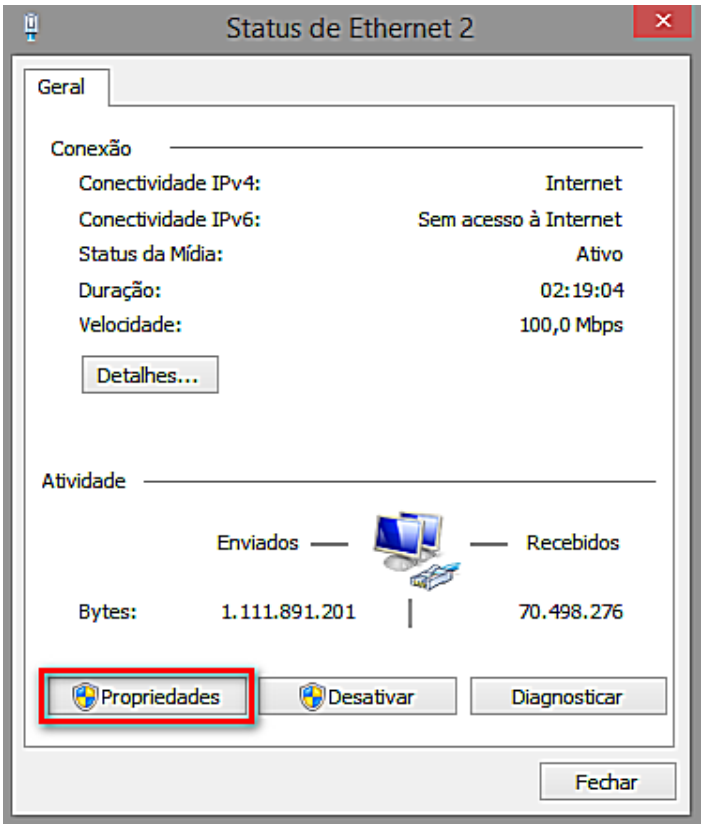


Figura 17 - Propriedades de conexão local

Na janela de propriedades do adaptador de rede, clique em '**Protocolo TCP/IP versão 4 (TCP/IPv4)'.**

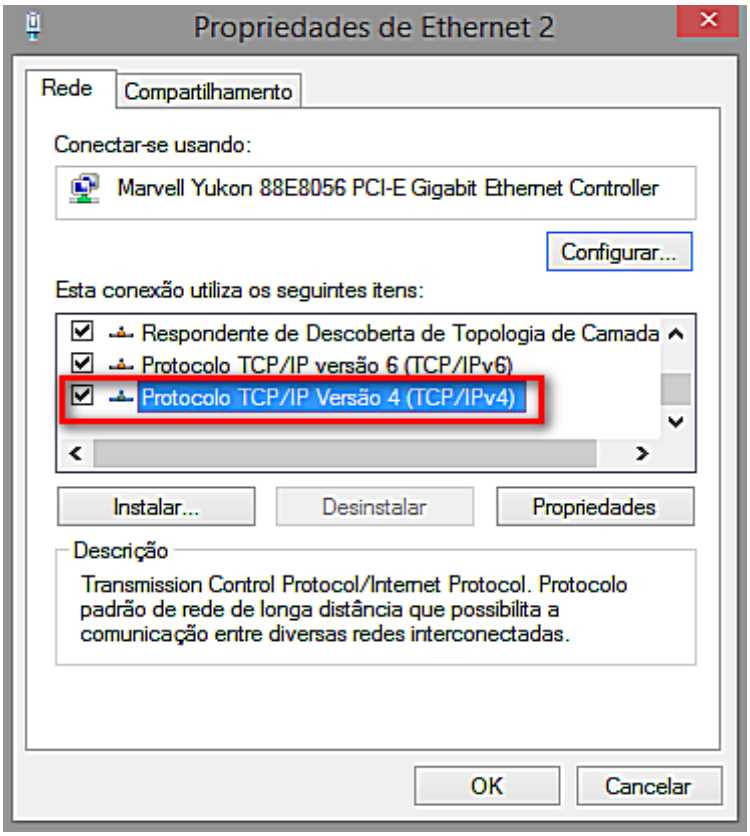


Figura 18 - Propriedades do adaptador de rede

Na janela de propriedades do protocolo TCP/IP, clique em '**Avançado...".**

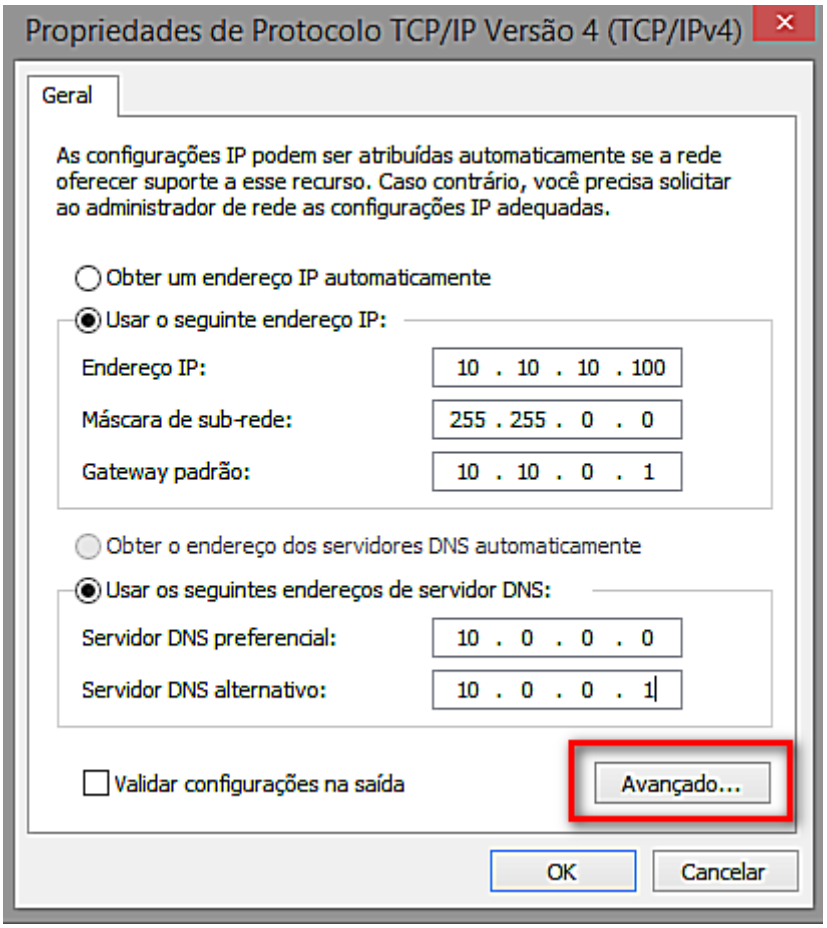

Propriedades de Protocolo TCP/IP Versão 4 (TCP/IPv4)
Geral
As configurações IP podem ser atribuídas automaticamente se a rede oferecer suporte a esse recurso. Caso contrário, você precisa solicitar ao administrador de rede as configurações IP adequadas.
Obter um endereço IP automaticamente
Usar o seguinte endereço IP:
Endereço IP: 10 . 10 . 10 . 100
Máscara de sub-rede: 255 . 255 . 0 . 0
Gateway padrão: 10 . 10 . 0 . 1
Obter o endereço dos servidores DNS automaticamente
Usar os seguintes endereços de servidor DNS:
Servidor DNS preferencial: 10 . 0 . 0 . 0
Servidor DNS alternativo: 10 . 0 . 0 . 1
Validar configurações na saída
Avançado...
OK
Cancelar

Figura 19 - Protocolo TCP/IP

Em seguida clique em '**Adicionar**'.

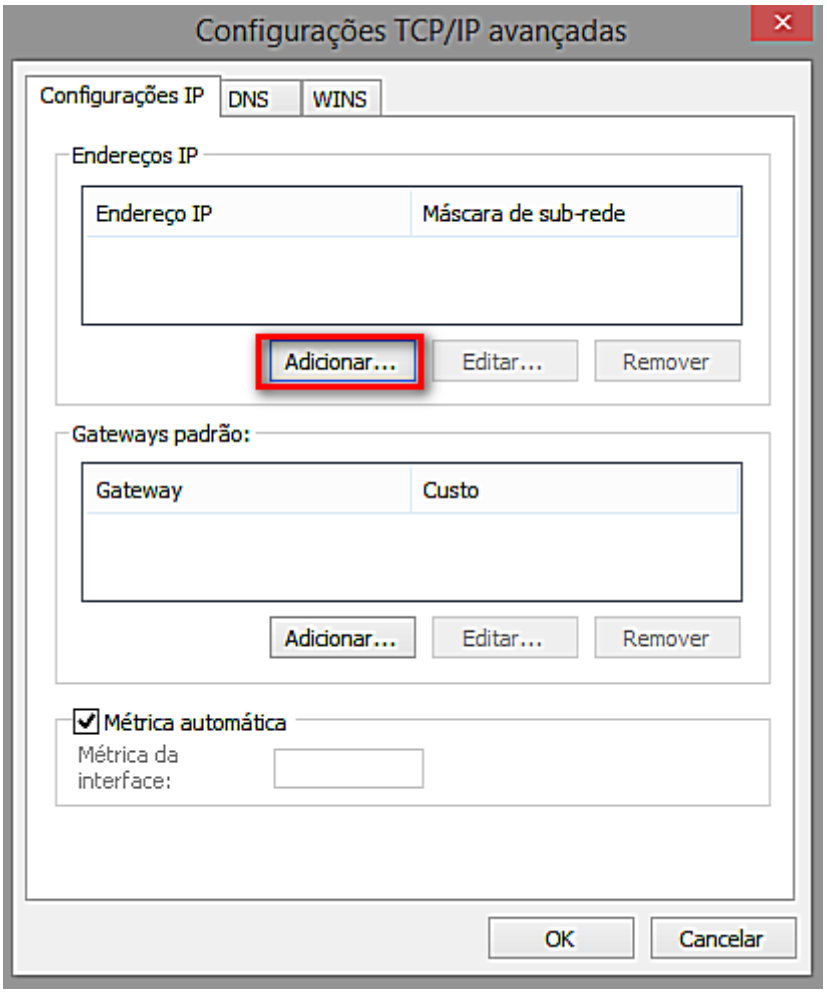


Figura 20 - Configurações avançadas

Insira o endereço IP – 192.168.0.102 e a mascara de rede 255.255.255.0, e clique em 'Adicionar'.

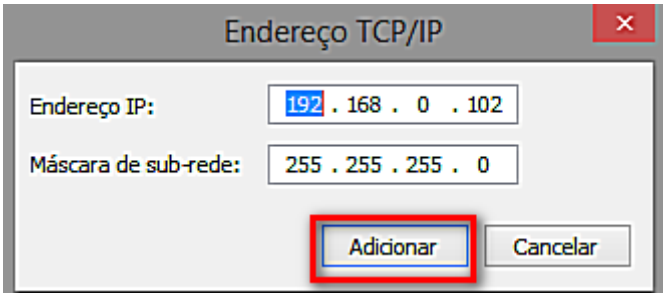


Figura 21 - Endereço TCP/IP

Ao concluir as definições acima, clique em 'OK' e abra seu browser.

Em seu browser acesse o endereço: https://192.168.0.100:8051

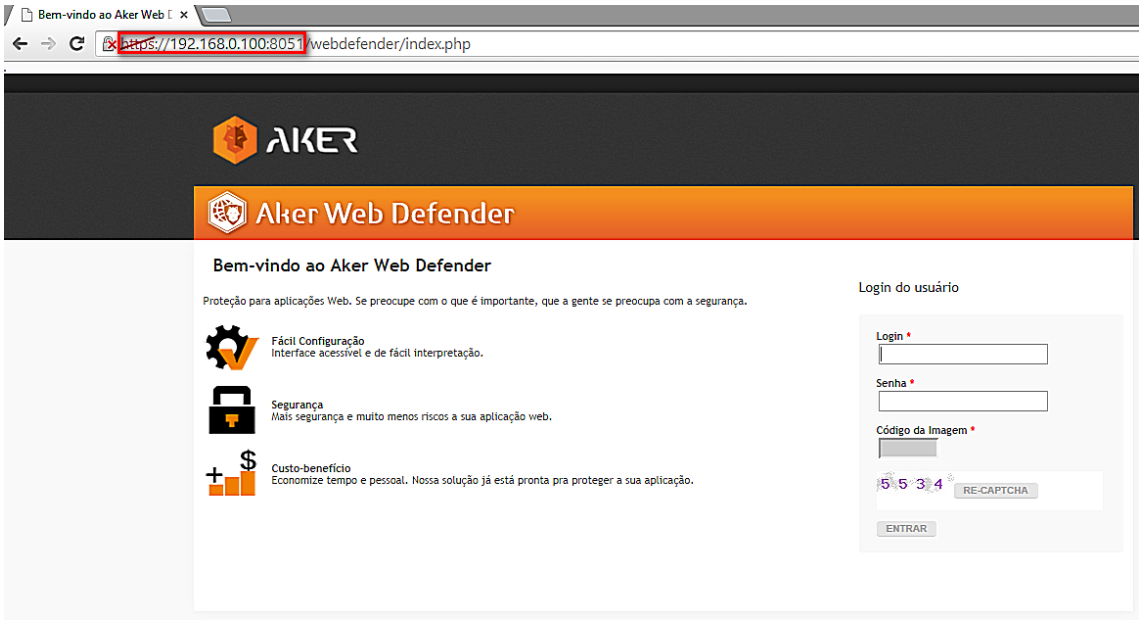
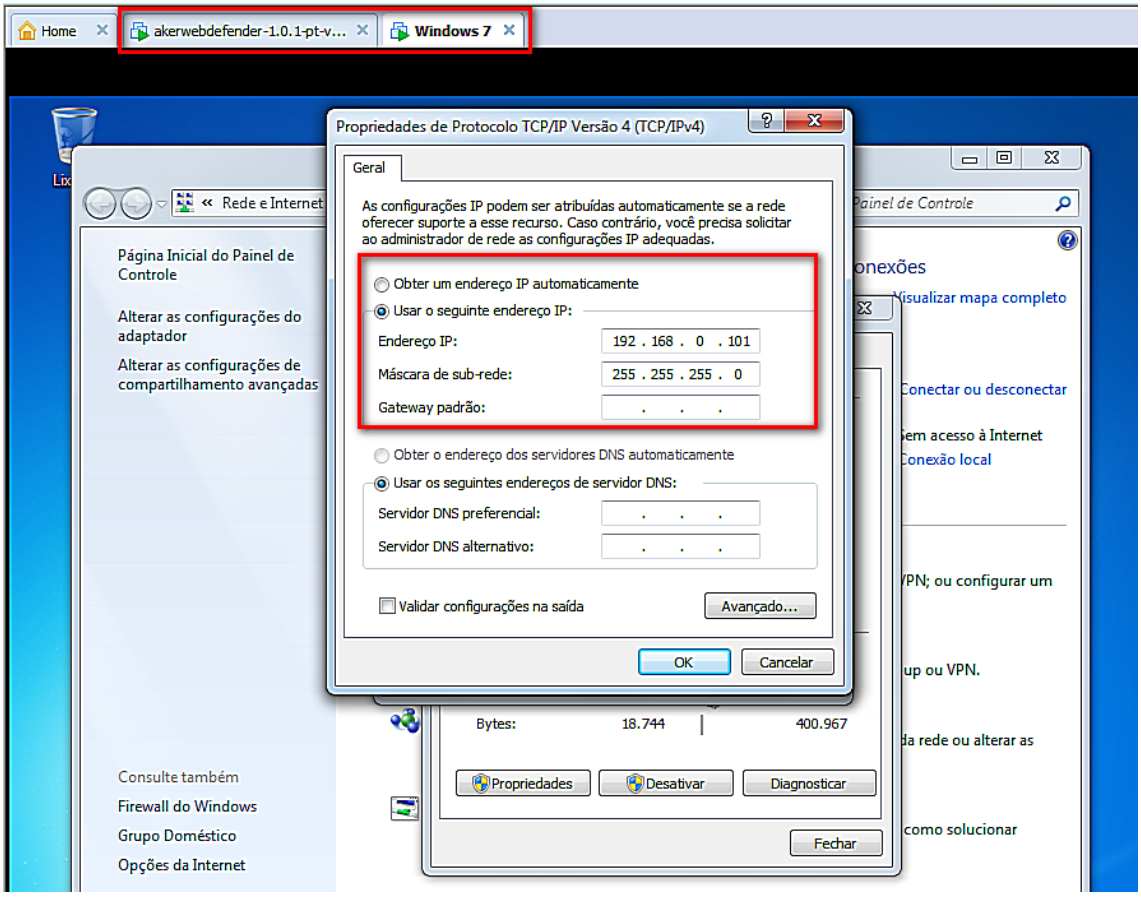

Bem-vindo ao Aker Web D
https://192.168.0.100:8051/webdefender/index.php
AKER
Aker Web Defender
Bem-vindo ao Aker Web Defender
Proteção para aplicações Web. Se preocupe com o que é importante, que a gente se preocupa com a segurança.
Fácil Configuração
Interface acessível e de fácil interpretação.
Segurança
Mais segurança e muito menos riscos a sua aplicação web.
Custo-benefício
Economize tempo e pessoal. Nossa solução já está pronta pra proteger a sua aplicação.
Login do usuário
Login *
Senha *
Código da Imagem *
RE-CAPTCHA
ENTRAR

Figura 22 - tela inicial do Aker Web Defender

Também é possível acessar o Aker Web Defender (VM) por meio de outra maquina virtual (ex: Windows xp, 7, 8, etc) que esteja no mesmo seguimento de rede. Para isso se deve configurar a interface de rede como no exemplo abaixo:


Home
akerwebdefender-1.0.1-pt-v...
Windows 7
Propriedades de Protocolo TCP/IP Versão 4 (TCP/IPv4)
Geral
As configurações IP podem ser atribuídas automaticamente se a rede oferecer suporte a esse recurso. Caso contrário, você precisa solicitar ao administrador de rede as configurações IP adequadas.
Obter um endereço IP automaticamente
Usar o seguinte endereço IP:
Endereço IP: 192 . 168 . 0 . 101
Máscara de sub-rede: 255 . 255 . 255 . 0
Gateway padrão:
Obter o endereço dos servidores DNS automaticamente
Usar os seguintes endereços de servidor DNS:
Servidor DNS preferencial:
Servidor DNS alternativo:
Validar configurações na saída
Avançado...
OK
Cancelar
Rede e Internet
Página Inicial do Painel de Controle
Alterar as configurações do adaptador
Alterar as configurações de compartilhamento avançadas
Consulte também
Firewall do Windows
Grupo Doméstico
Opções da Internet
Bytes: 18.744 400.967
Propriedades
Desativar
Diagnosticar
Fechar

Endereço IP: 192.168.0.101

Máscara de sub-rede: 255.255.255.0

Clique em '**ok**'.

Abra o browser, e acesse o endereço: https://192.168.0.100:8051/

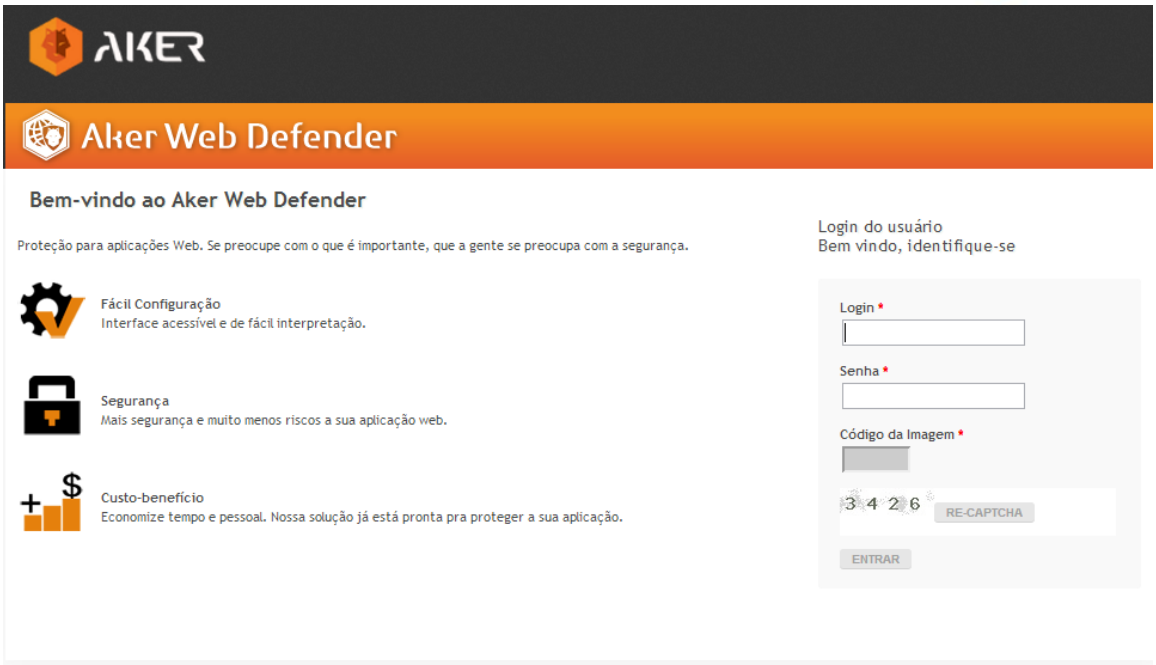

AKER
Aker Web Defender
Bem-vindo ao Aker Web Defender
Proteção para aplicações Web. Se preocupe com o que é importante, que a gente se preocupa com a segurança.
Fácil Configuração
Interface acessível e de fácil interpretação.
Segurança
Mais segurança e muito menos riscos a sua aplicação web.
Custo-benefício
Economize tempo e pessoal. Nossa solução já está pronta pra proteger a sua aplicação.
Login do usuário
Bem vindo, identifique-se
Login *
Senha *
Código da Imagem *
3 4 2 6
RE-CAPTCHA
ENTRAR

Figura 23 - Tela de acesso do Aker Web Defender

A segurança de acesso às informações do **Aker Web Defender** é realizada perante a solicitação da identificação e senha.

Inicialmente o usuário Administrador deve entrar com a senha padrão e criar os usuários do sistema e seus privilégios.

Usuário: admin

Senha padrão: **WebDefender**

****** Mude a senha do administrador no primeiro acesso.***

A configuração da Propriedade de Vídeo sugerida é 1024x768 nos navegadores Firefox e chrome;

2.6. Sessão

Sessão é o período de tempo que o sistema disponibiliza para que você utilize o **Aker Web Defender**. A sessão é iniciada após a validação da sua identificação no sistema.

Enquanto você estiver interagindo com o **Aker Web Defender**, o tempo disponível é ilimitado. Caso não esteja utilizando o **Aker Web Defender**, este fechará sua sessão por meio de um processo de Time out.

Enquanto você estiver em uma sessão todos os processos que você realizar serão registrados. Portanto, nunca deixe uma sessão aberta no seu micro computador, pois alguém pode alterar alguma configuração usando o seu usuário. Pelo mesmo motivo, nunca forneça sua senha a ninguém.

O sistema controla o tempo de inatividade da sessão por meio de um "***timer***", que especifica o tempo máximo que você pode ficar sem fazer nenhuma interação com o sistema.

Se você ficar mais tempo que o determinado sem utilizar o **Aker Web Defender**, este automaticamente encerra a sessão, obrigando-o a identificar-se novamente.

2.7. Painel de Controle

O *Painel de controle* do **Aker Web Defender** permite que o usuário visualize o **menu de configurações do sistema**, **incidentes, relatórios, gerencie usuários e mude configurações**. O *Painel de controle* também exibe o uso de "***CPU, Memória, Tráfego das interfaces de rede e Hora atual do Aker Web Defender***". Na visualização de "***Incidentes***" podemos ver os detalhes dos ataques detectados, como exibido nas imagens a seguir:

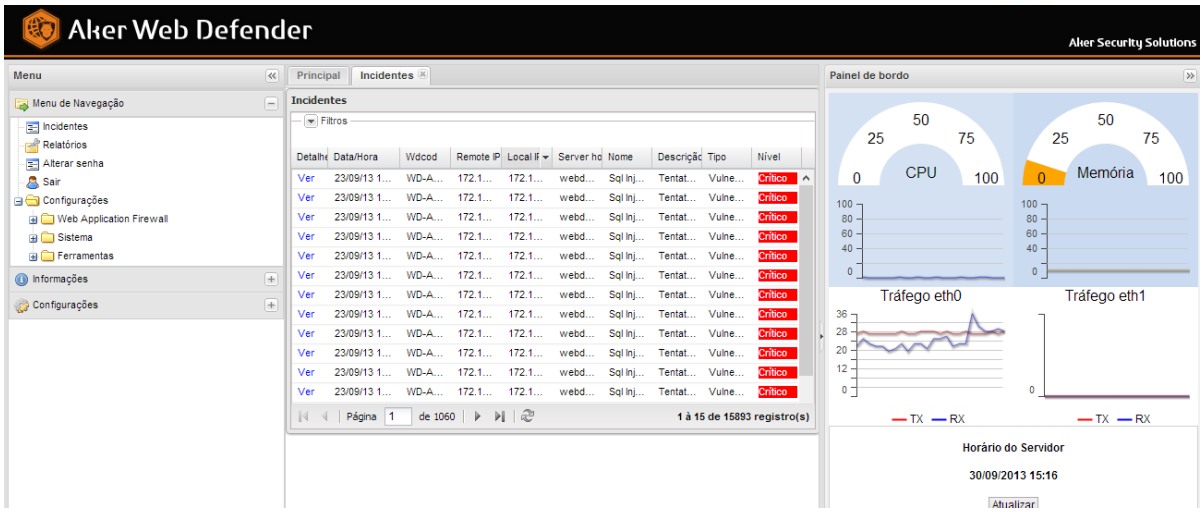


Figura 24 - Painel de controle

Menus

3. Menus

A barra de menu do **Aker Web Defender** e localizada no lado esquerdo da tela principal. Este menu permite que o usuário tenha acesso à todas as funcionalidades do **Aker Web Defender**, facilitando a interação do usuário com o sistema. A seguir mais informações sobre os menus do **Aker Web Defender**.

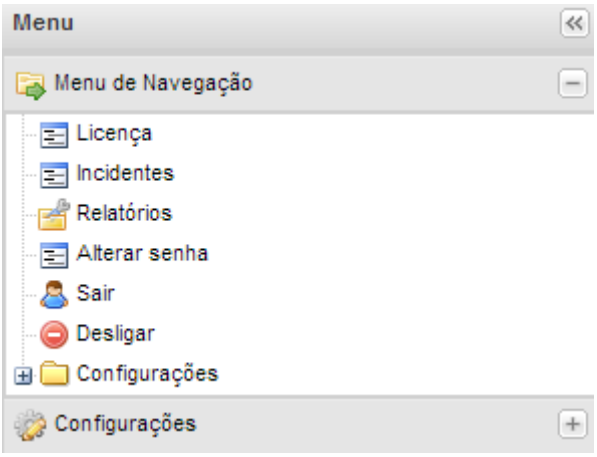


Figura 25 - Menus

3.1. Licença

Por meio desta janela o usuário deve ativar sua licença do Aker Web Defender, definir um e-mail que receberá notificações quando a licença estiver prestes a expirar. Nesta janela também é possível visualizar as informações sobre a sua licença atual.

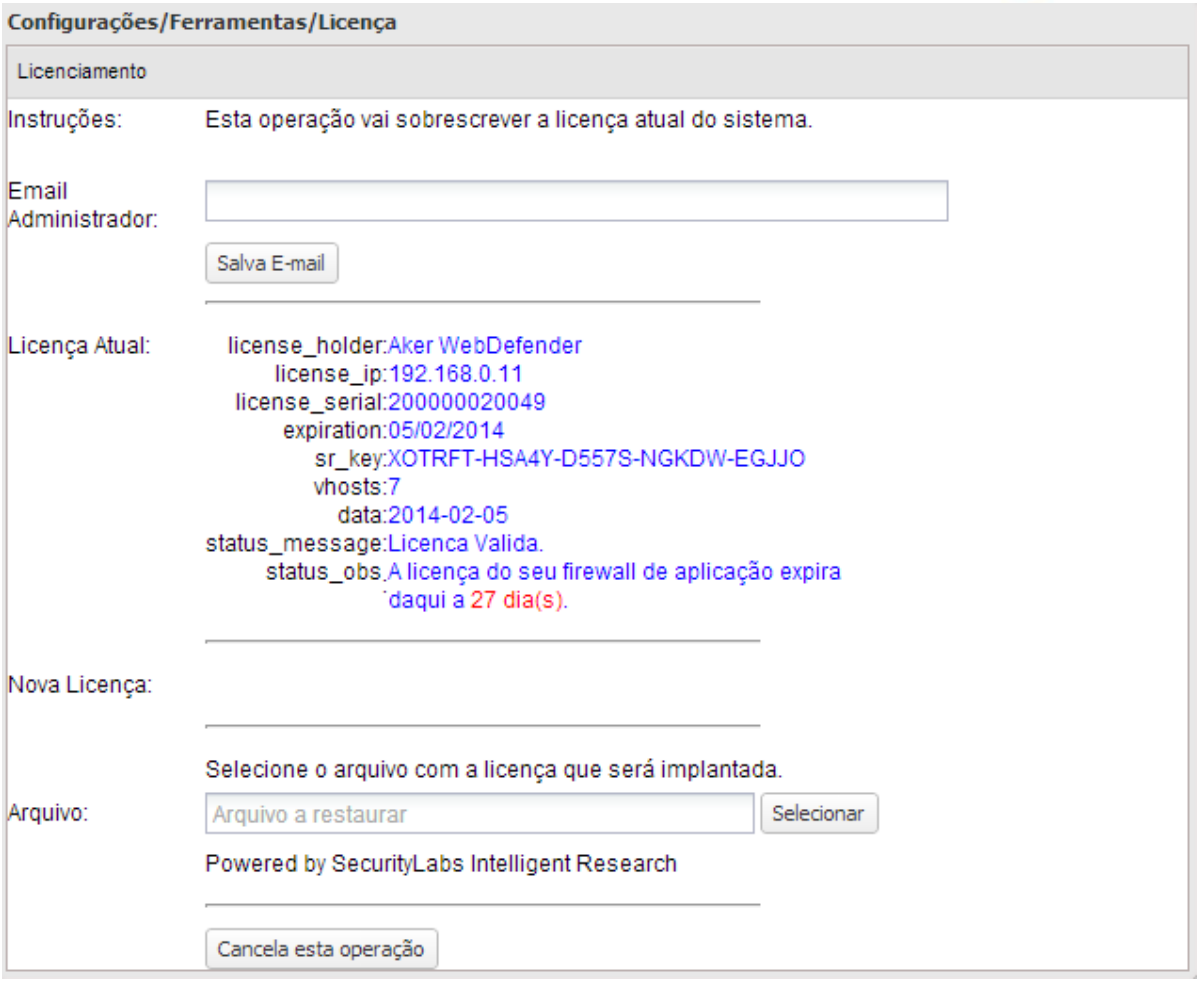


Figura 26 - Licença

E-mail Administrador: Neste campo o usuário deve definir o e-mail que receberá notificações do Aker Web Defender, por exemplo, quando a licença estiver prestes a expirar o sistema irá enviar notificações para o e-mail definido.

Licença Atual: Exibe as informações da licença atual.

Arquivo: Permite que o usuário selecione o local que o arquivo de sua licença está armazenado para que a licença seja ativada.

Ao selecionar a licença, clique em "**Salvar**" para completar a operação.

3.2. Incidentes

O módulo incidentes é a tela principal do **Aker Web Defender**, nela o usuário pode visualizar as ações (bloqueios) realizadas pelo **Aker Web Defender** quando algum código malicioso for enviado para os servidores Web.

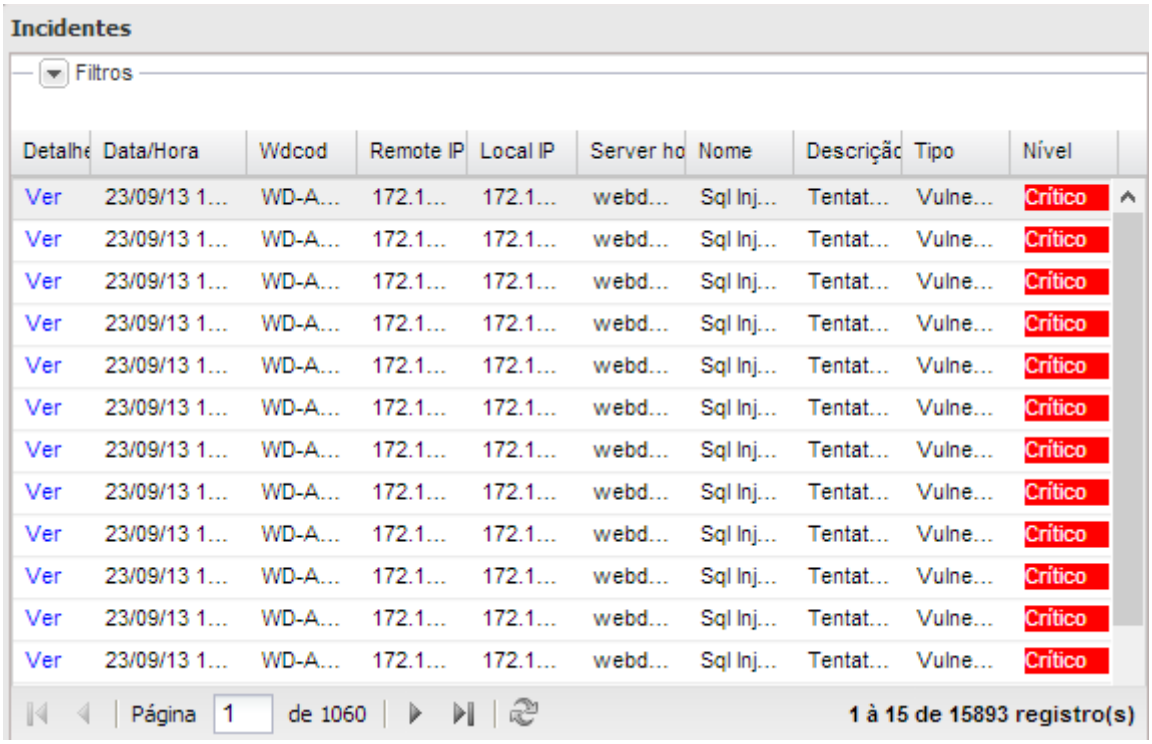

Incidentes
Filtros
Detalhe Data/Hora Wdcod Remote IP Local IP Server ho Nome Descriçã Tipo Nível
Ver 23/09/13 1... WD-A... 172.1... 172.1... webd... Sql Inj... Tentat... Vulne... Crítico
Página 1 de 1060
1 à 15 de 15893 registro(s)

Figura 27 - Aba incidentes

- **Filtros**

Por meio desta opção é possível efetuar filtragens selecionado os "***Dados do Ataque***, ***Período, IP remoto, IP local, Site atacado e Tipo de ataque***" desejados.

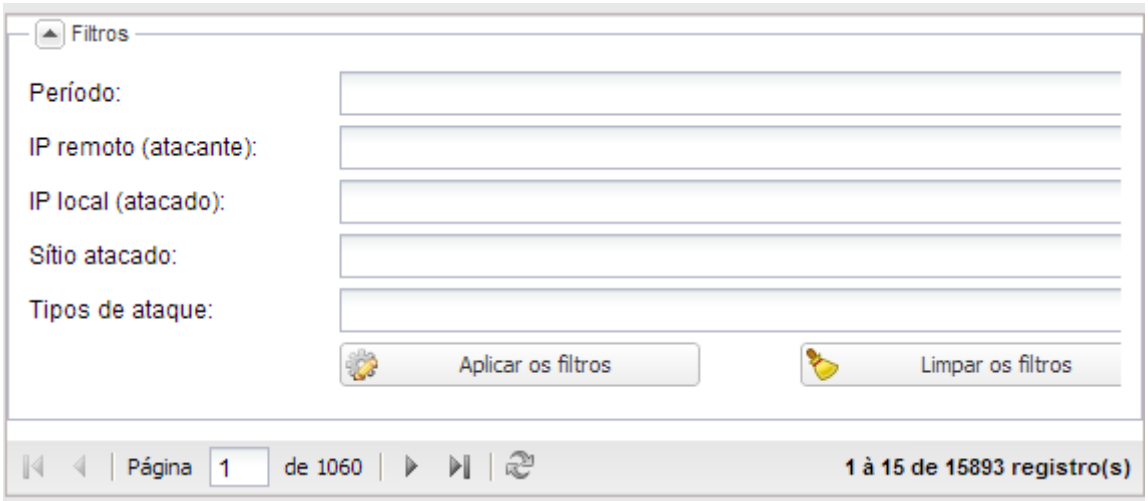
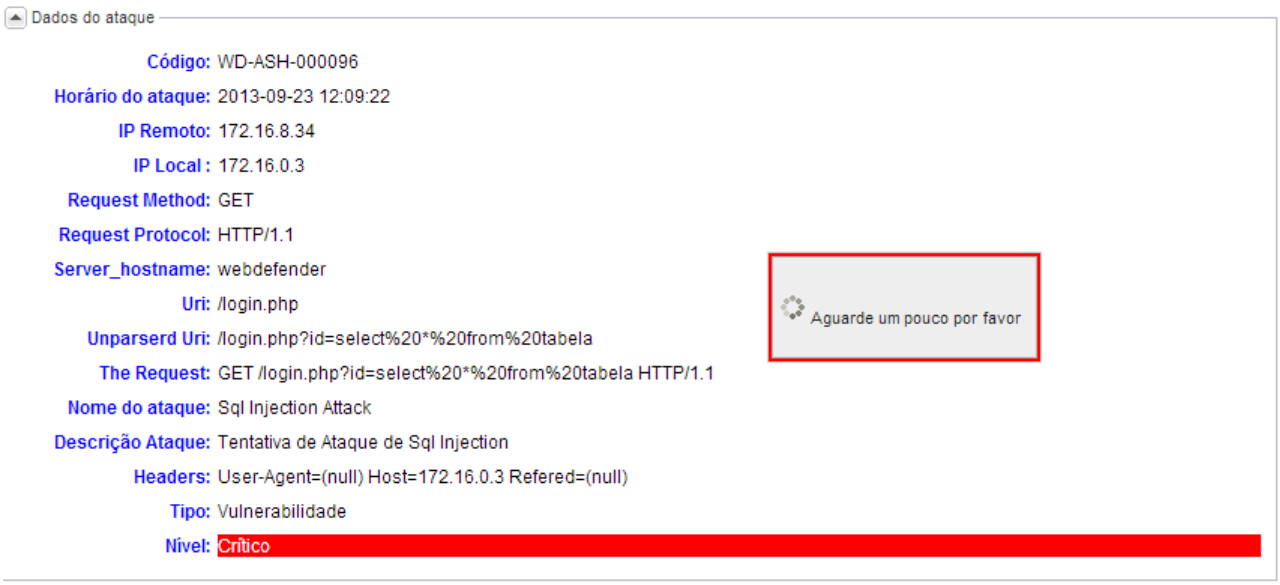


Figura 28 - Filtragem de Incidentes

- **Detalhe**

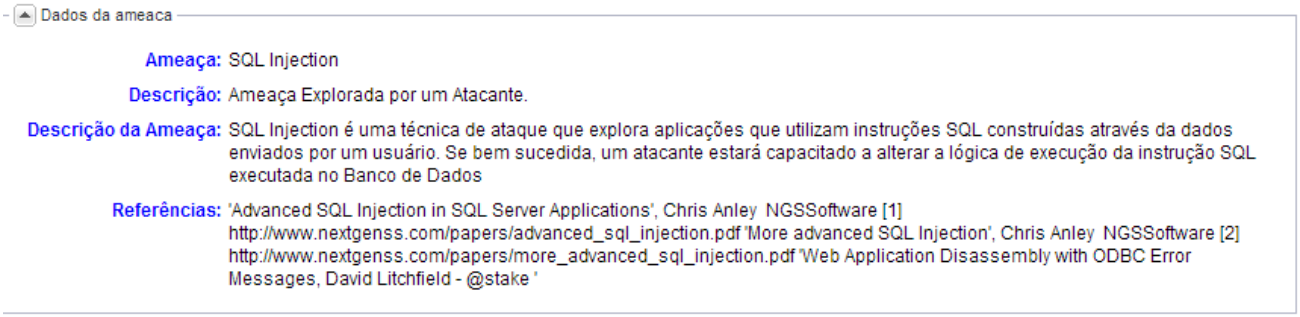
Por meio desta coluna o usuário pode visualizar dados específicos do ataque desejado, para visualizar estes dados clique na opção (Ver).

➢ **Dados do ataque:** Exibe informações técnicas sobre o ataque como qual assinatura foi usada no ataque, horário, IP local e remoto, e etc.

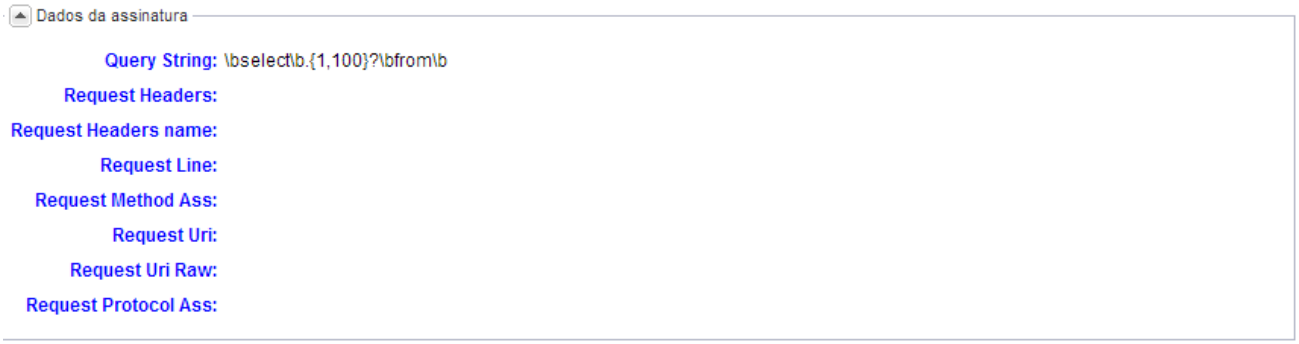


➢ **Estatística do ataque:** Exibe datas, horários e quantidade de ataques.

➢ **Dados da ameaça:** Exibe detalhes sobre o tipo de ataque usado.


Dados da ameaca
Ameaça: SQL Injection
Descrição: Ameaça Explorada por um Atacante.
Descrição da Ameaça: SQL Injection é uma técnica de ataque que explora aplicações que utilizam instruções SQL construídas através da dados enviados por um usuário. Se bem sucedida, um atacante estará capacitado a alterar a lógica de execução da instrução SQL executada no Banco de Dados
Referências: 'Advanced SQL Injection in SQL Server Applications', Chris Anley NGSSoftware [1] http://www.nextgenss.com/papers/advanced_sql_injection.pdf 'More advanced SQL Injection', Chris Anley NGSSoftware [2] http://www.nextgenss.com/papers/more_advanced_sql_injection.pdf 'Web Application Disassembly with ODBC Error Messages, David Litchfield - @stake '

- **Dados da assinatura:** Exibe os dados da assinatura que foi utilizada para detectar o ataque.



- **Data/Hora**

Esta coluna exibe a data e o horário do ataque.

- **Wdcod**

Esta coluna exibe qual o tipo de assinatura que foi usada.

- **Remote IP**

Esta coluna exibe o IP Remoto do atacante.

- **Local IP**

Esta coluna exibe o IP local do atacante.

- **Sever hostname**

Esta coluna exibe o domínio que foi atacado.

- **Nome**

Esta coluna exibe o nome do ataque detectado.

- **Descrição**

Esta coluna exibe uma breve descrição do ataque detectado.

- **Tipo**

Esta coluna informa o tipo do ataque.

- **Nível**

Esta coluna informa qual o nível do ataque.

3.3. Relatórios

O módulo "**Relatório**" permite que o usuário emita relatórios contendo informações sobre os incidentes detectados.

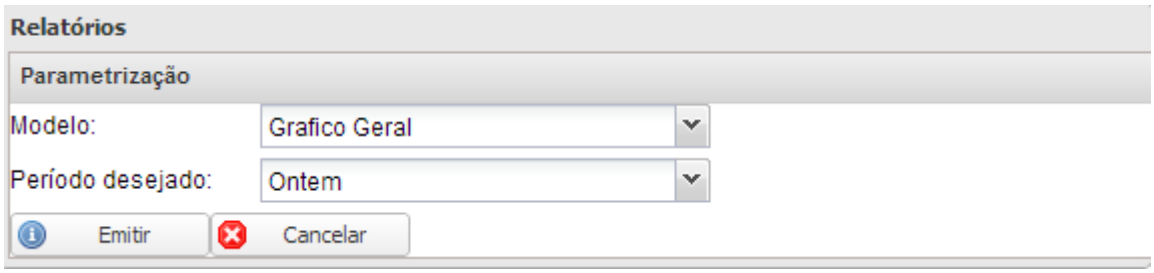


Figura 29 - Módulo "Relatórios"

Modelo: Permite que o usuário selecione o modelo que o relatório será gerado, as opções disponíveis são: Gráfico Geral, Histograma e Relação.

Período desejado: Permite que o usuário selecione o período em que o relatório será gerado, as opções disponíveis são: Hoje, Ontem, Esta semana, Semana passada, Este mês, Este ano, Ano passado, e específico.

3.4. Alterar Senha

O módulo "**Alterar Senha**" permite que os usuários alterem suas próprias senhas de acesso ao **Aker Web Defender**.

Os usuários devem estar previamente cadastrados no sistema.

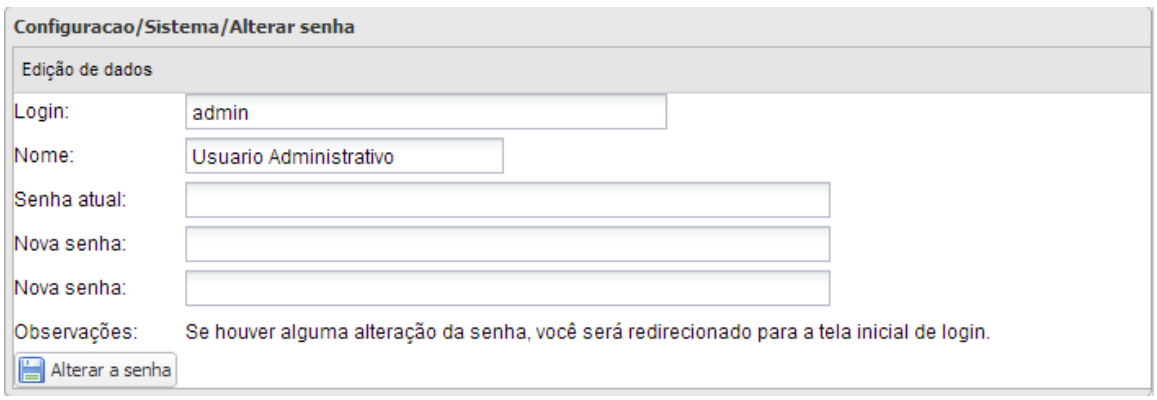
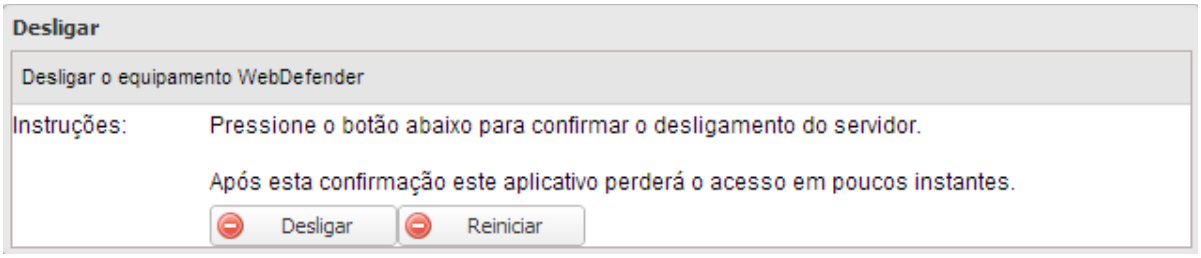


Figura 30 - Módulo "Alterar Senha"

3.5. Desligar

Esta opção permite que o usuário encerre sua sessão e desligue a máquina.


Desligar
Desligar o equipamento WebDefender
Instruções:
Pressione o botão abaixo para confirmar o desligamento do servidor.
Após esta confirmação este aplicativo perderá o acesso em poucos instantes.
Desligar
Reiniciar

3.6. Sair

Para sair de uma sessão se deve clicar no botão "***Sair*** ", desta forma, o usuário sairá do **Aker Web Defender,** e continuará com o browser ativo.

Se você clicar no controle "***Fechar***" do browser, você não encerra a sessão, apenas o browser.

Qualquer outra forma de encerrá-lo, como por exemplo, desligar o computador, é chamada de encerramento anormal.

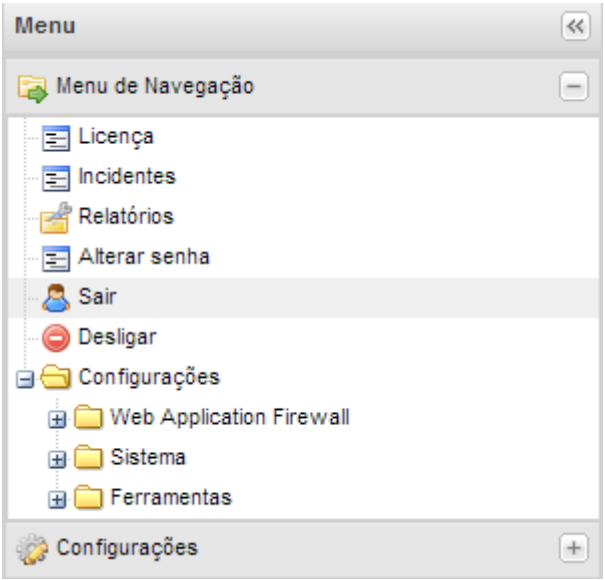


Figura 31 - Menu de Opções do Aker Web Defender

Módulo Configurações

4. Módulo Configurações

No módulo Configurações são encontradas as configurações do "***Web Application Firewall, Sistema e Ferramentas***". Mais detalhes sobre estas configurações serão exibidos a seguir.

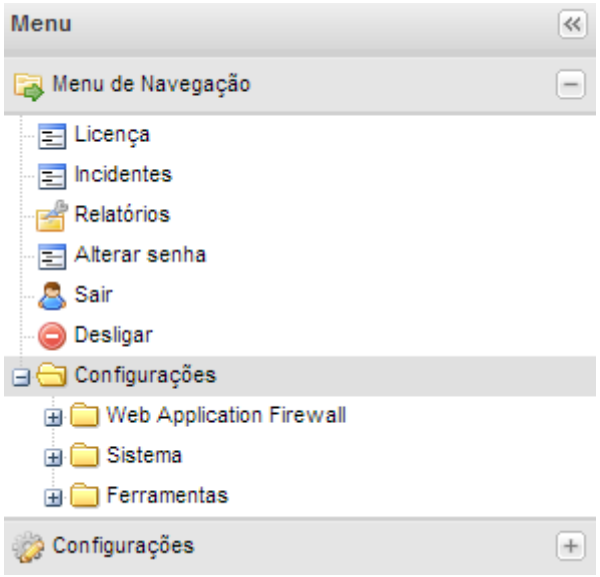


Figura 32 - Módulo Configurações

4.1. Web Application Firewall

O módulo "**Web Application Firewall"** permite que o usuário configure servidores, certificados digitais, sítios virtuais, IPs e portas entre outros. Mais informações sobre este módulo serão exibidas a seguir:

Figura 33 - Web Application Firewall

4.2. Servidores Reais

Por meio da aba "***Configurações -> Web Application Firewall -> Servidores Reais***" é possível *configurar/incluir* servidores reais com seus respectivos IPs e portas de acesso a aplicação Web.

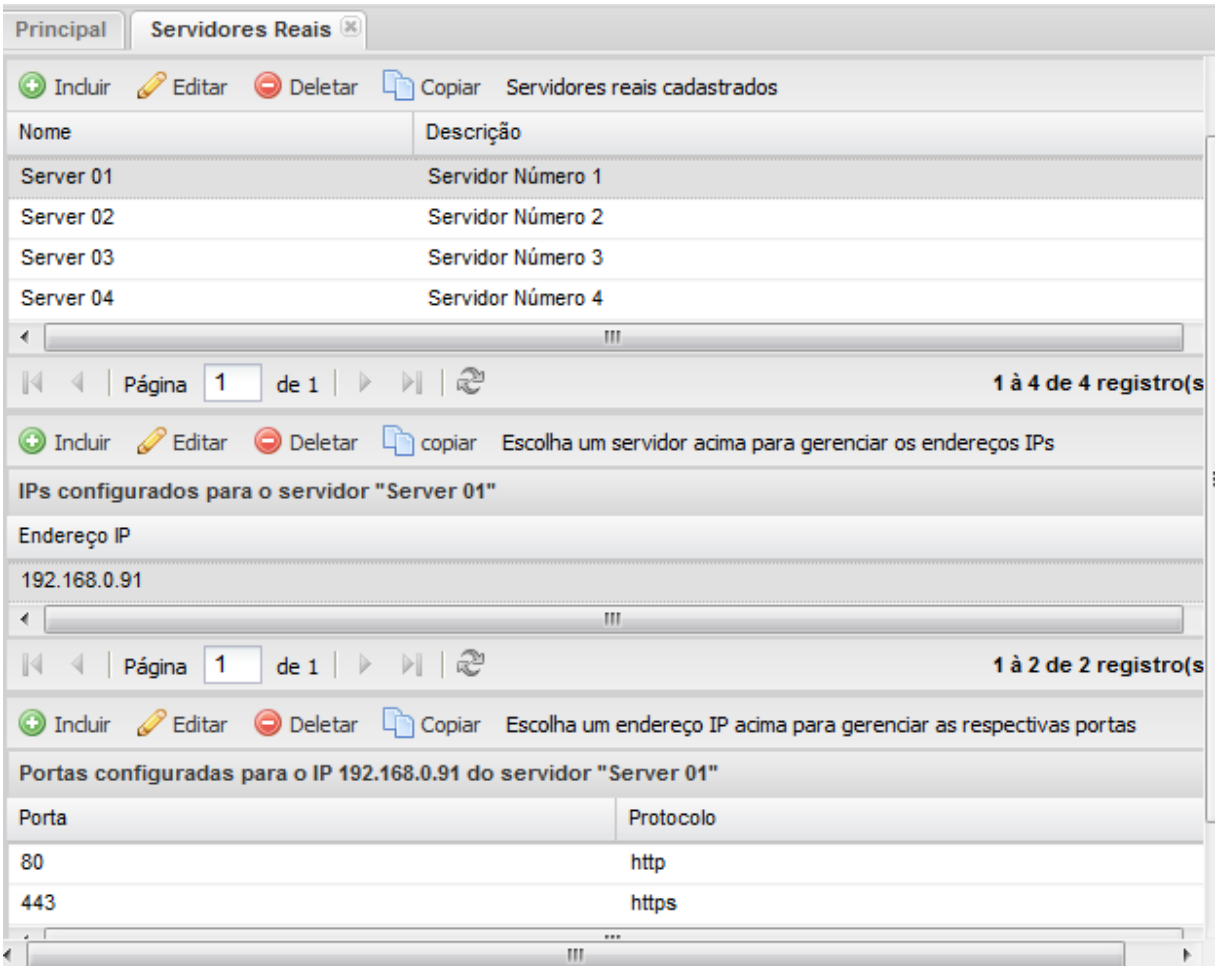


Figura 34 - Aba Servidores Reais

4.2.1 Incluindo um novo Servidor Real

Para incluir um novo Servidor Real siga os passos a seguir:

- Na aba "***Servidores Reais***" clique no botão "***Incluir***".
- Digite o nome do servidor (**Ex: Pluton**) e digite a descrição do servidor (***Ex: Dell Power Edge 410***).
- Clique no botão "***Incluir***"

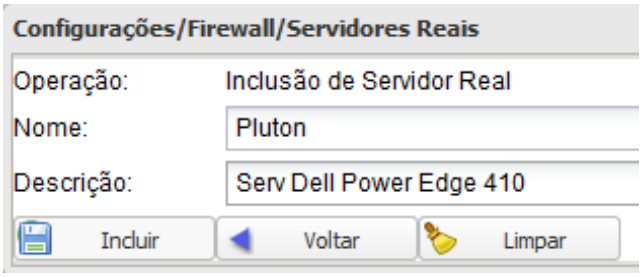


Figura 35 - Servidor Real

4.2.2 Incluindo o IP do Servidor Real

Para incluir o IP do Servidor Real siga os passos a seguir:

- Na aba "***Servidores Reais***" selecione o servidor real (***Ex: Pluton***), em seguida clique no botão "***Incluir***" endereço IP.
- Digite o número IP real do servidor (***Ex: 192.168.0.241***).
- Clique no botão "***Incluir***".

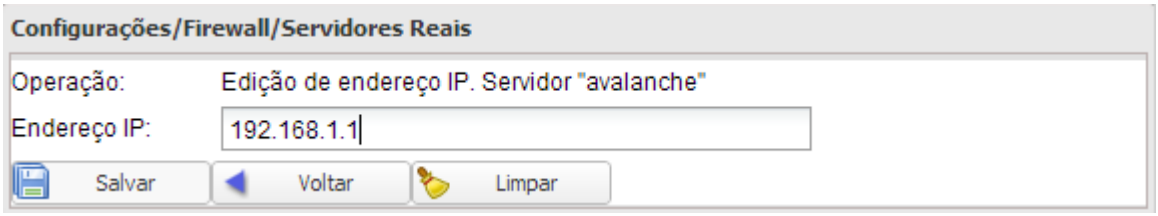


Figura 36 - Incluindo o IP do Servidor Real

4.2.3 Incluindo a porta do Servidor Real

Para inserir a porta do Servidor Real siga os passo a seguir:

- Na aba "***Servidores Reais***" selecione o servidor real (***Ex: Pluton***), em seguida selecione o IP do servidor real (Ex***: 192.168.0.241***), em seguida clique no botão "***Incluir***" porta.

  Digite ou escolha a porta (***Ex: 80***) a ser utilizada pelo servidor real e o protocolo (***Ex: HTTP***).
- Clique no botão "***Incluir***".

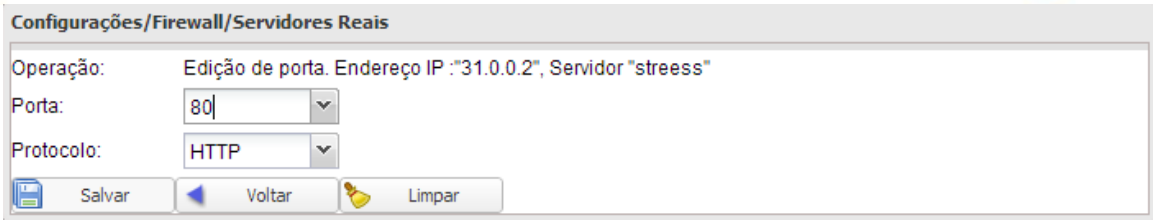


Figura 37 - Incluindo a porta do Servidor Real

4.3. Virtual Hosts

Esta aba permite que o usuário configure, inclua, ou delete os **Virtual hosts**.

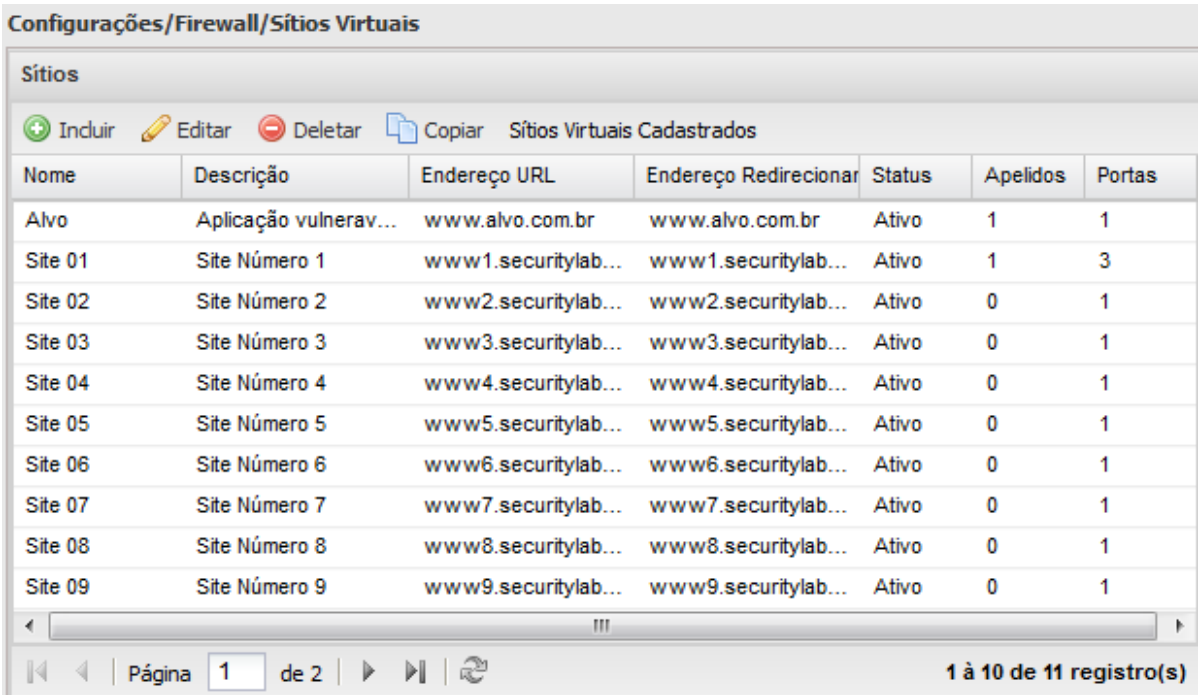


Figura 38 - Sítios Virtuais

4.3.1 Incluindo um novo Sitio Virtual (Virtual Host)

Para incluir um novo Sitio Virtual siga os passos a seguir:

- Em "**Virtual Hosts**" clique no botão "***Incluir***".

A imagem abaixo será exibida:

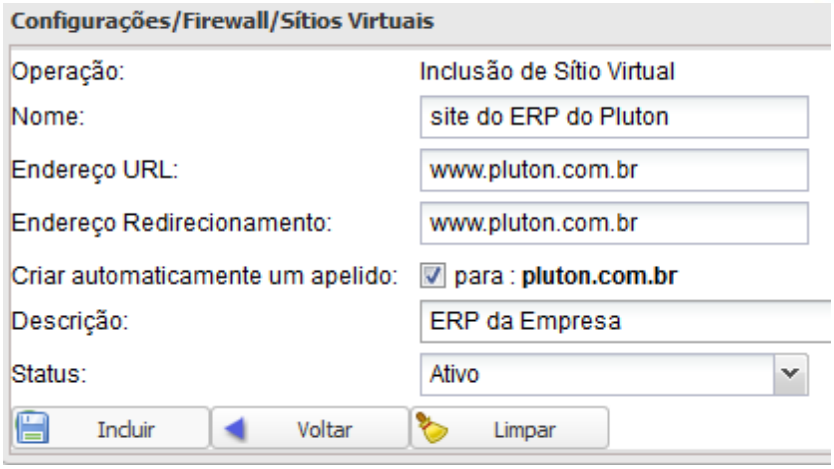


Figura 39 - Incluindo Sítios Virtuais

- Digite o nome do site (Ex: Site do ERP Pluton) e digite a "***URL***" de acesso ao site (Ex: www.pluton.com.br).
- Em "***Endereço Redirecionamento***" digite para onde você quer que seja encaminhado o atacante após a detecção da tentativa de intrusão (Ex: Neste caso estamos redirecionando para a index do www.pluton.com.br).
- Em "***Descrição***" digite uma descrição para o site.
- Em "***Status***" marque "***Ativo***" para ativar o site.
- Clique no botão "***Incluir***".

4.3.2 Configurando Portas e Aliases para o novo Sitio Virtual

Ao incluir o novo Sitio Virtual siga os passo a seguir para configurar uma porta ou Aliases para o novo Sitio Virtual:

- Por meio da aba "***Configurações -> Web Application Firewall -> Servidores Virtuais -> Sítios***" clique no site a ser configurado (Ex: www.pluton.com.br), observe as aba "***Aliases e Portas***" na parte inferior da tela.

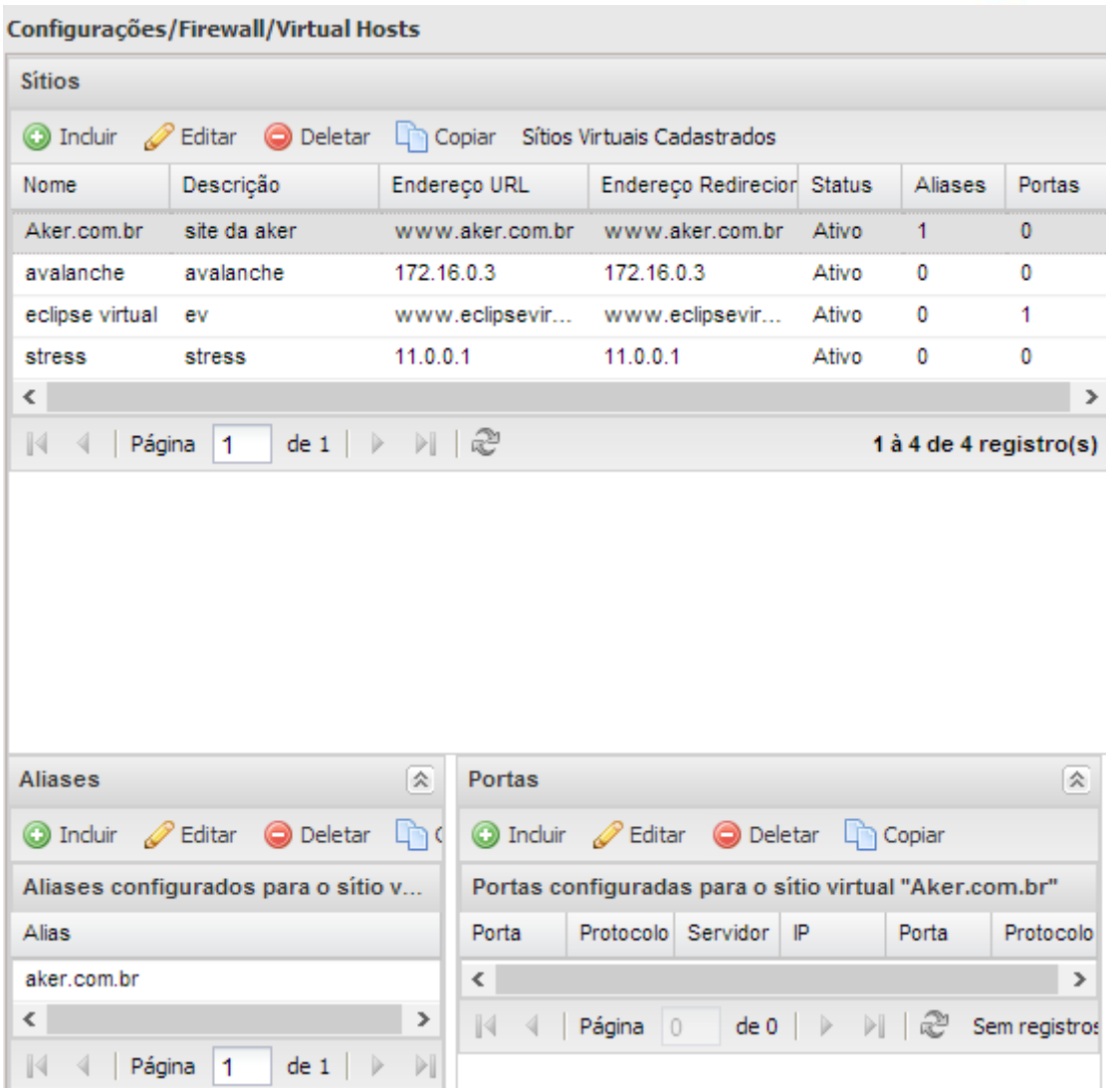


Figura 40 - Aba Aliases e Portas

- Na aba "***Aliases***" podemos cadastrar o apelido do site e na aba "***Portas***" os dados de "***Porta, Protocolo, Servidor Real e endereço IP***" do servidor conforme a tela abaixo:

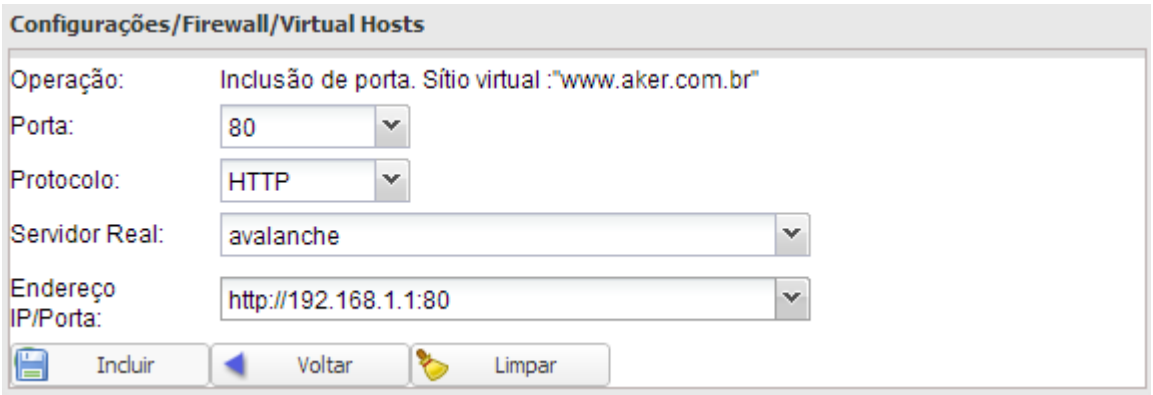


Figura 41 - Aba Porta

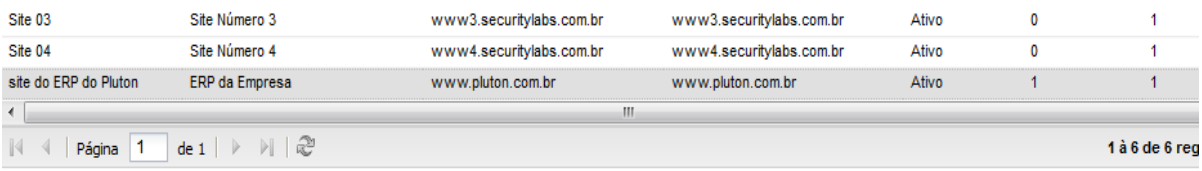
Porta: Neste caso será a porta de comunicação utilizada pelo browser do cliente.

Protocolo: Neste caso será o protocolo de comunicação utilizado pelo browser do cliente.

Servidor Real: Host (nome) definido na criação do servidor real

Endereço IP/Porta: Dados definidos na criação do servidor real.

Figura 42 - Aba Aliases


Site 03 Site Número 3 www3.securitylabs.com.br www3.securitylabs.com.br Ativo 0 1
Site 04 Site Número 4 www4.securitylabs.com.br www4.securitylabs.com.br Ativo 0 1
site do ERP do Pluton ERP da Empresa www.pluton.com.br www.pluton.com.br Ativo 1 1
Página 1 de 1
1 à 6 de 6 reg

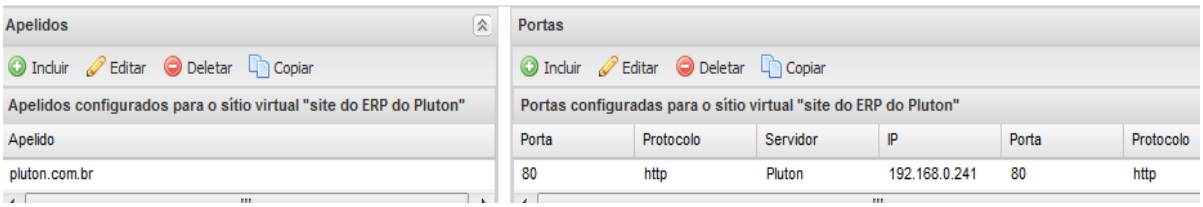

Apelidos
Incluir Editar Deletar Copiar
Apelidos configurados para o sítio virtual "site do ERP do Pluton"
Apelido
pluton.com.br
Portas
Incluir Editar Deletar Copiar
Portas configuradas para o sítio virtual "site do ERP do Pluton"
Porta Protocolo Servidor IP Porta Protocolo
80 http Pluton 192.168.0.241 80 http

Figura 43 - Definindo Apelido

4.4. Assinaturas

No módulo "***Assinaturas***" podemos visualizar todas às assinaturas cadastradas no **Aker Web Defender** para detecção de ataques.

Entende-se detecção de ataques por assinatura as atividades do sistema procurando por eventos que correspondam a padrões pré-definidos de ataques e outras atividades maliciosas.

Estes padrões são conhecidos como assinaturas e geralmente cada assinatura corresponde a um ataque.

No módulo Assinaturas, existem 04 (quatro) itens para detecção de ataques e 01 (um) item denominado Whitelist para liberação de falsos positivos sendo: ***"Conexão, Headers, RequestBody, ResponseBody e Whitelist***".

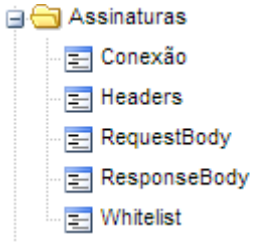


Figura 44 - Assinaturas

Conexão: Esta assinatura tem como objetivo identificar dados oriundos da conexão, como: valor de IP, sessão e nome de usuário.

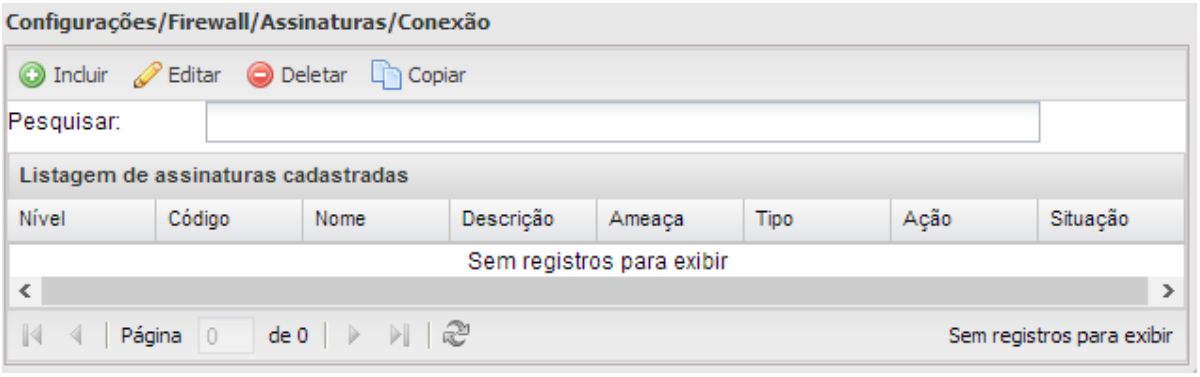


Figura 45 - Assinaturas (conexão)

Headers: Esta assinatura tem como objetivo Identificar dados do cabeçalho HTTP, como método, URI, versão, outros.

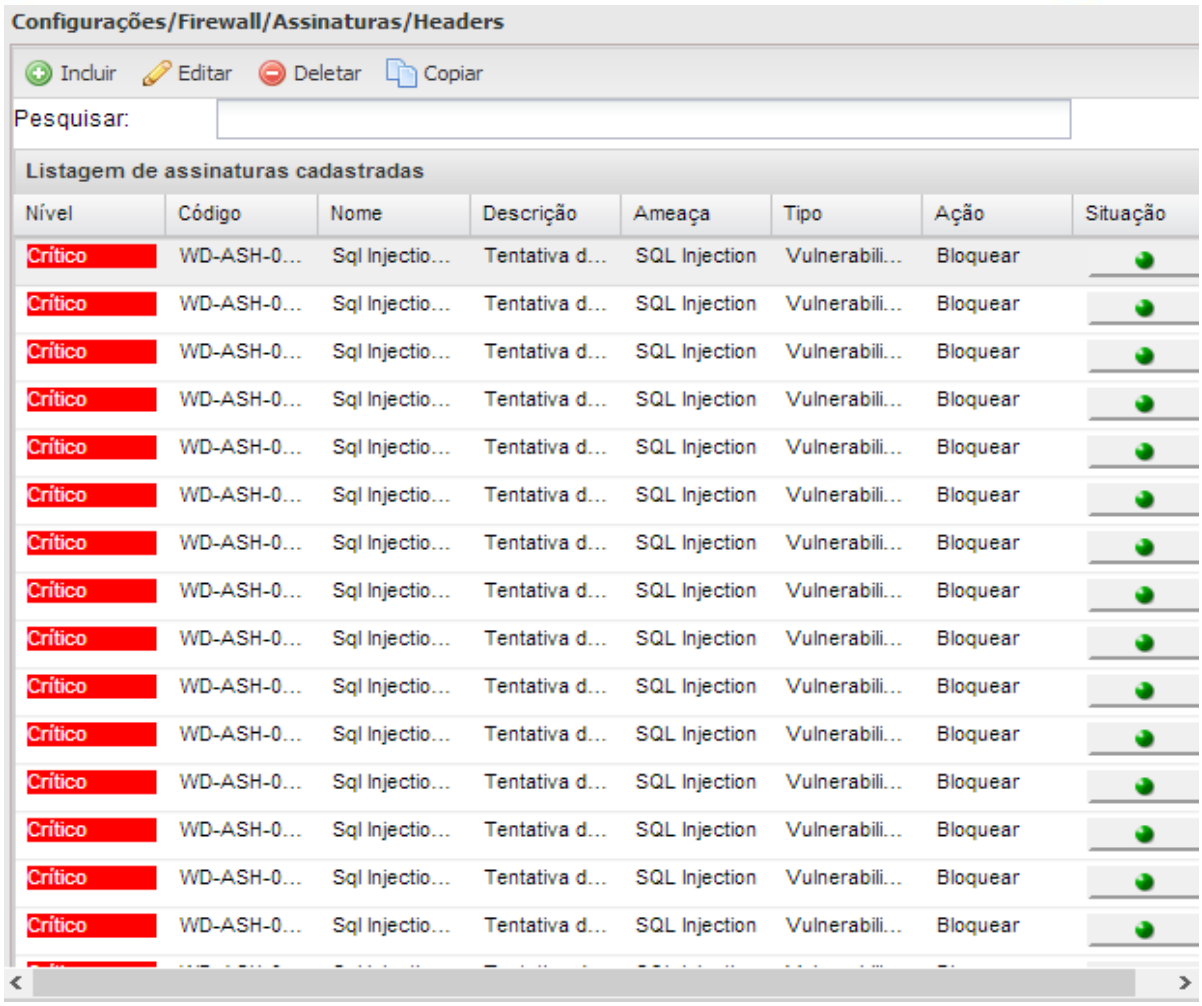


Figura 46 - Assinaturas (Headers)

RequestBody: Esta assinatura tem como objetivo Identificar dados do corpo de um pacote HTTP, como dados vindos de formulários e métodos *POST/PUT*.

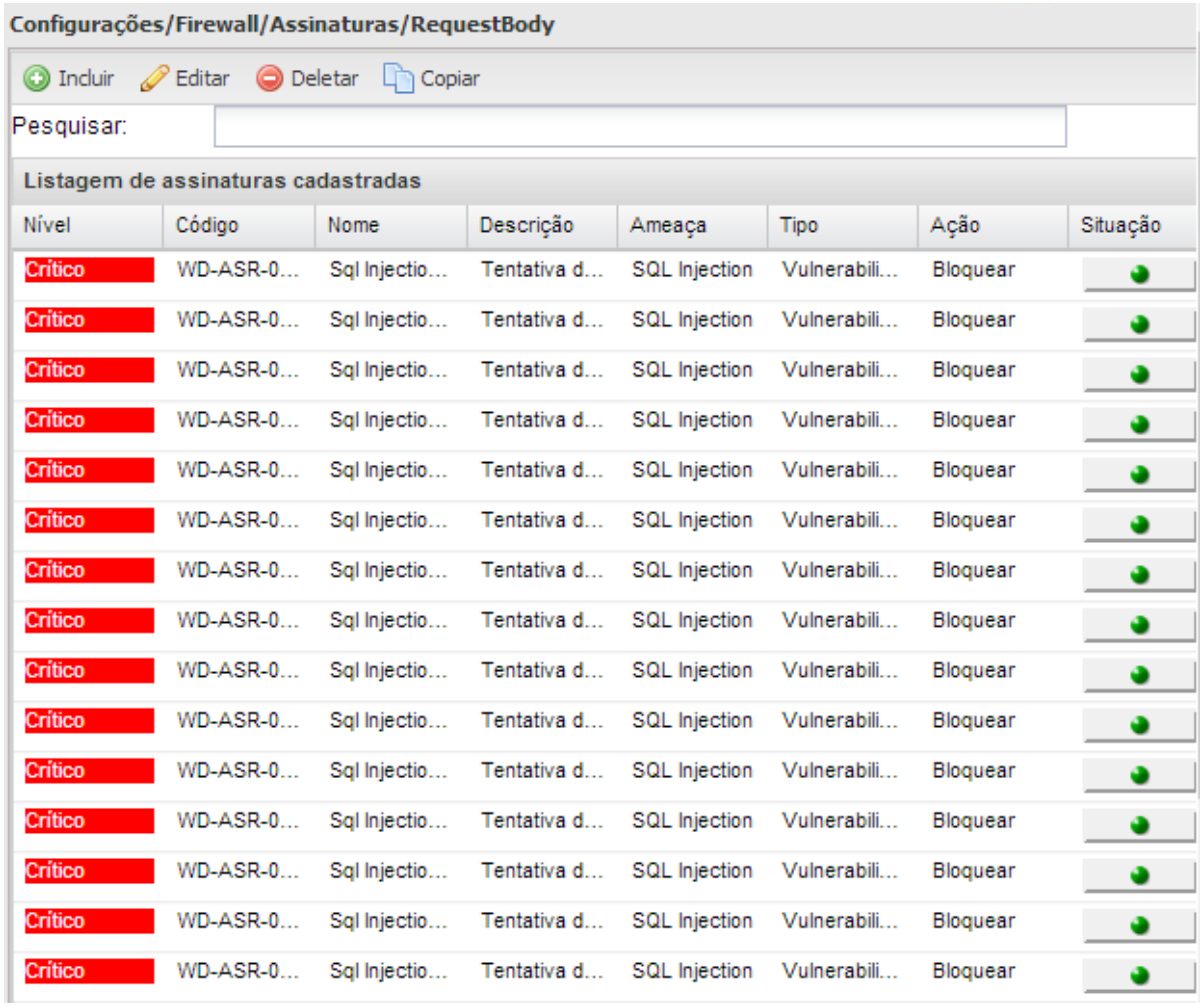


Figura 47 - Assinaturas (RequestBody)

ResponseBody: Esta assinatura tem como objetivo Identificar dados de resposta do servidor WEB, como página HTML, Cabeçalho de resposta, outros.

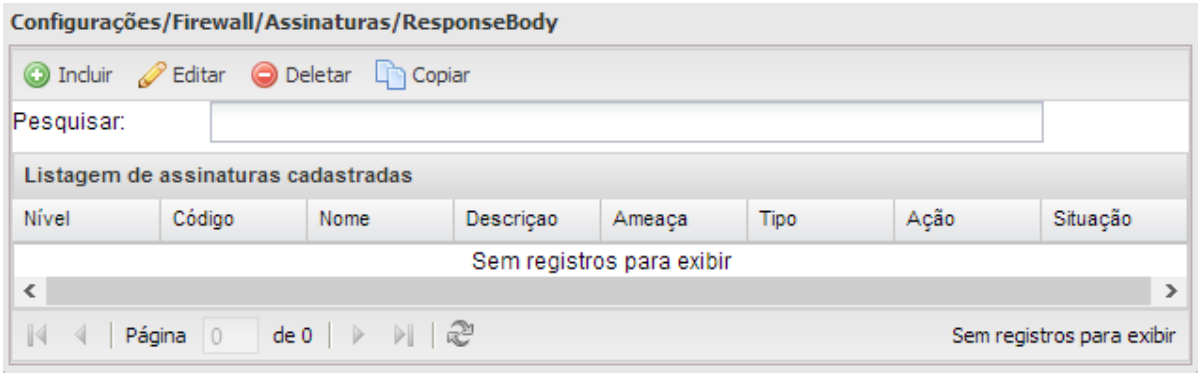


Figura 48 - Assinaturas (ResponseBody)

Whitelist: Esta assinatura tem como objetivo liberar o acesso a uma URL (uri) identificada e considerada maliciosa pelo sistema.

Figura 49 - Inserindo Assinatura na Whitelist

4.5. Aprendizado

O módulo "**Aprendizado**" serve de suporte para o módulo "**Positivo**". Este módulo permite que o usuário, configure o sistema para que ele possa aprender como um site específico funciona. Desta forma o modo positivo ao detectar qualquer atividade, que seja diferente das atividades, que foram armazenadas pela configuração definida no módulo "**Aprendizado**" serão bloqueadas.

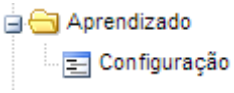


Figura 50 – Aprendizado

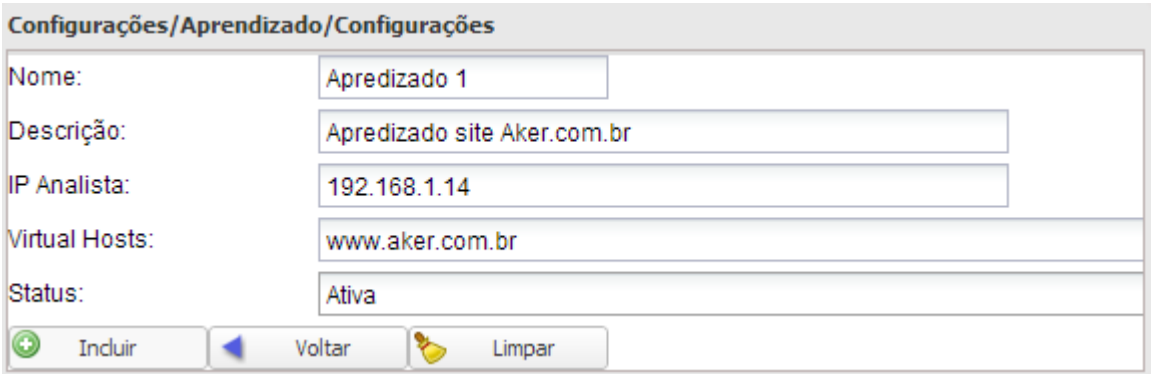


Figura 51 - Configurando o módulo Aprendizado

Nome: Define o nome da configuração de aprendizado.

Descrição: Define uma descrição para esta configuração.

IP Analista: Define o IP do Analista o qual o sistema irá aprender o funcionamento do site desejado.

Virtual Hosts: Define o nome do site para o aprendizado.

Status: Define se esta configuração estará "**Ativa** ou **Inativa**".

Os módulos de "**Aprendizado**" e "**Positivo**" não podem funcionar simultaneamente, ou seja, é necessário que um dos dois módulos esteja ***desativado*** para que o outro funcione.

4.6. Positivo

No módulo "**Positivo**" o usuário vai definir quais regras armazenadas pelo módulo de "**Aprendizado**" serão permitidas, desta forma, definindo quais entradas, expressões e assinaturas que serão permitidas e quais serão bloqueadas.

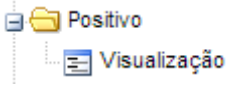


Figura 52 - Positivo

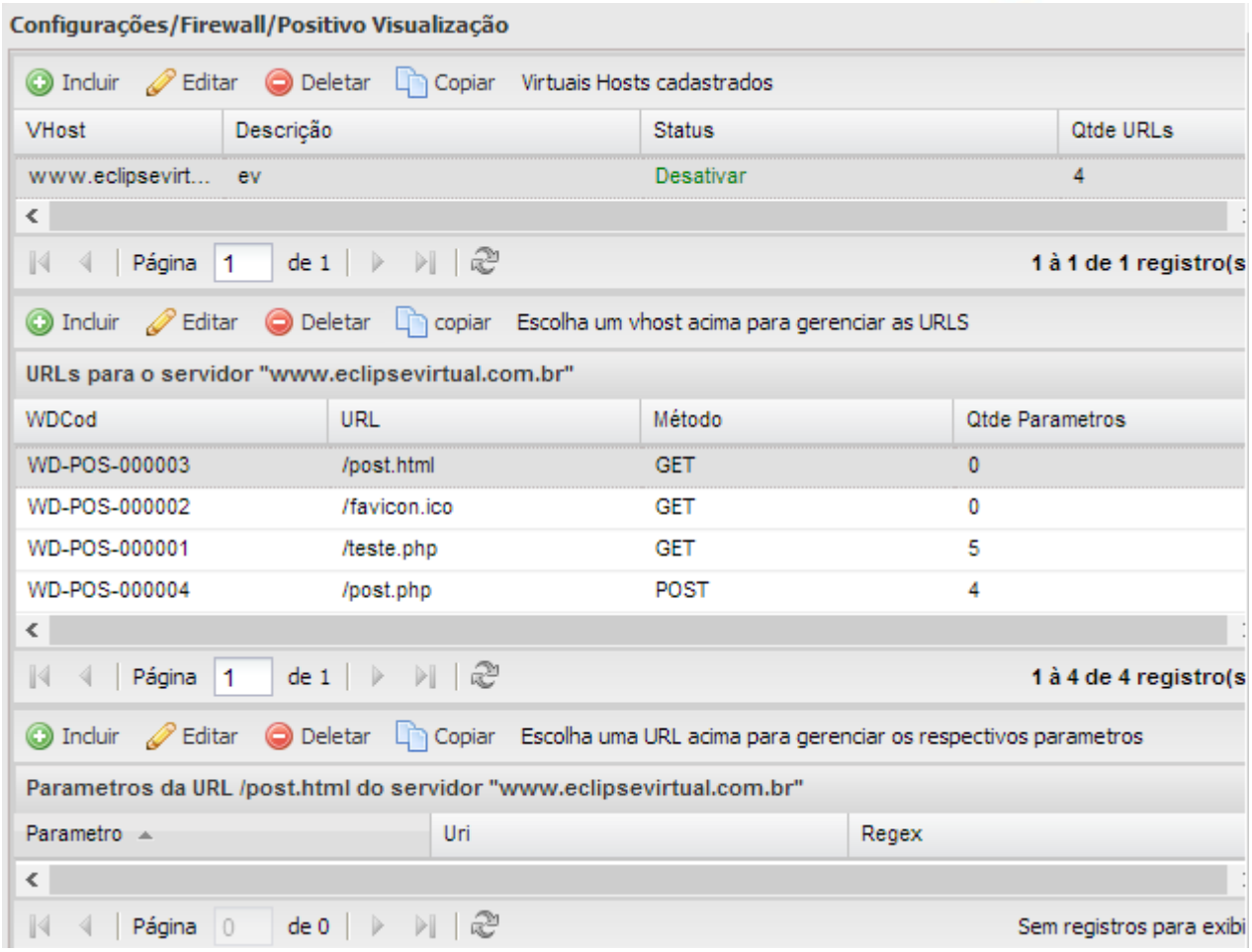

Configurações/Firewall/Positivo Visualização
Incluir Editar Deletar Copiar Virtuais Hosts cadastrados
VHost Descrição Status Qtde URLs
www.eclipsevirt... ev Desativar 4
Página 1 de 1 1 à 1 de 1 registro(s
Incluir Editar Deletar copiar Escolha um vhost acima para gerenciar as URLS
URLs para o servidor "www.eclipsevirtual.com.br"
WDCod URL Método Qtde Parametros
WD-POS-000003 /post.html GET 0
WD-POS-000002 /favicon.ico GET 0
WD-POS-000001 /teste.php GET 5
WD-POS-000004 /post.php POST 4
Página 1 de 1 1 à 4 de 4 registro(s
Incluir Editar Deletar Copiar Escolha uma URL acima para gerenciar os respectivos parametros
Parametros da URL /post.html do servidor "www.eclipsevirtual.com.br"
Parametro Uri Regex
Página 0 de 0 Sem registros para exibi

Figura 53 - módulo visualização

Para configurar o módulo Positivo siga o passos abaixo:

- Primeiro o usuário deve definir qual o host virtual previamente cadastrado será usado.

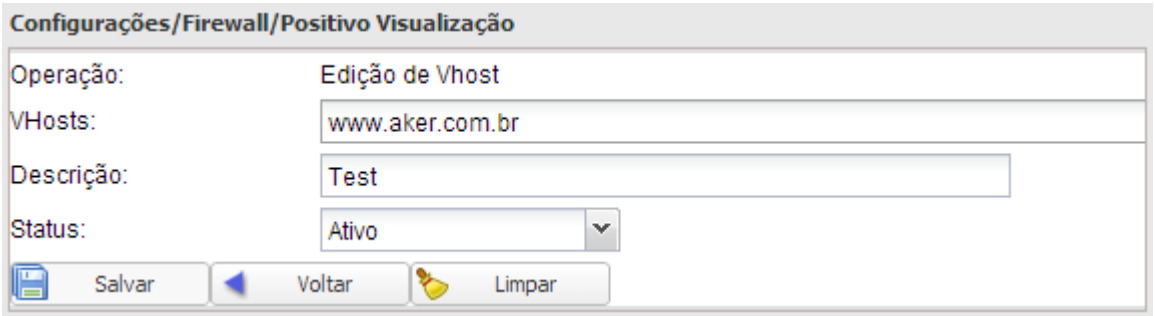


Figura 54 – Configurando do positivo de visualização

VHosts: Define qual o host virtual que será usado.

Descrição: Define uma descrição para esta configuração.

Status: Define se esta configuração estará "**Ativa** ou **Inativa**"

4.7. Inteligência Artificial

O módulo "**Inteligência Artificial**" permite que o usuário configure as ações dos detectores de ataques, permitindo que o sistema execute estas ações automaticamente.

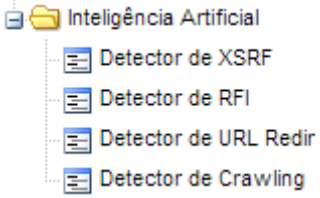


Figura 55 - Inteligência Artificial

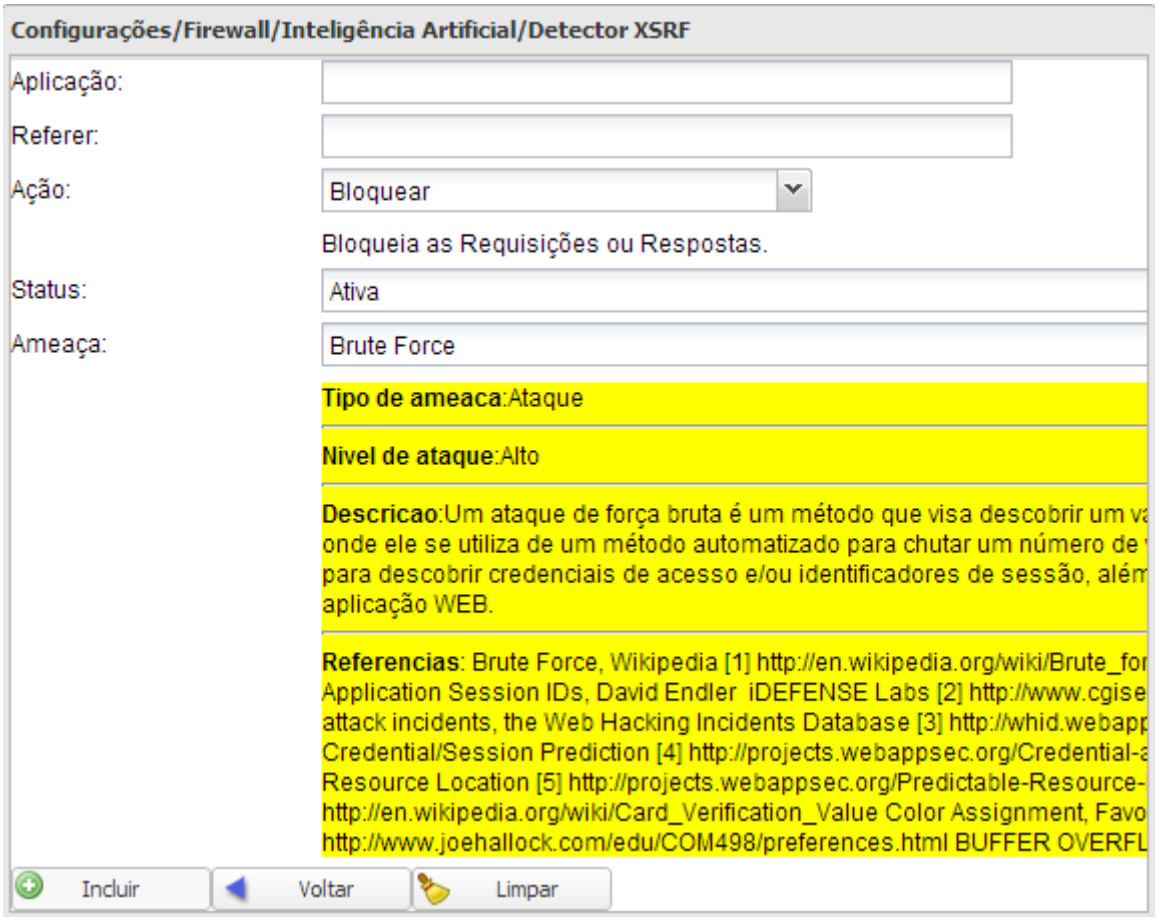

Configurações/Firewall/Inteligência Artificial/Detector XSRF
Aplicação:
Referer:
Ação:
Bloquear
Bloqueia as Requisições ou Respostas.
Status:
Ativa
Ameaça:
Brute Force
Tipo de ameaca:Ataque
Nivel de ataque:Alto
Descricao:Um ataque de força bruta é um método que visa descobrir um va
onde ele se utiliza de um método automatizado para chutar um número de
para descobrir credenciais de acesso e/ou identificadores de sessão, além
aplicação WEB.
Referencias: Brute Force, Wikipedia [1] http://en.wikipedia.org/wiki/Brute_for
Application Session IDs, David Endler iDEFENSE Labs [2] http://www.cgise
attack incidents, the Web Hacking Incidents Database [3] http://whid.webapp
Credential/Session Prediction [4] http://projects.webappsec.org/Credential-a
Resource Location [5] http://projects.webappsec.org/Predictable-Resource-
http://en.wikipedia.org/wiki/Card_Verification_Value Color Assignment, Favo
http://www.joehallock.com/edu/COM498/preferences.html BUFFER OVERFL
Incluir
Voltar
Limpar

Figura 56 - Detector XSRF

Figura 57 - Opções de ataques

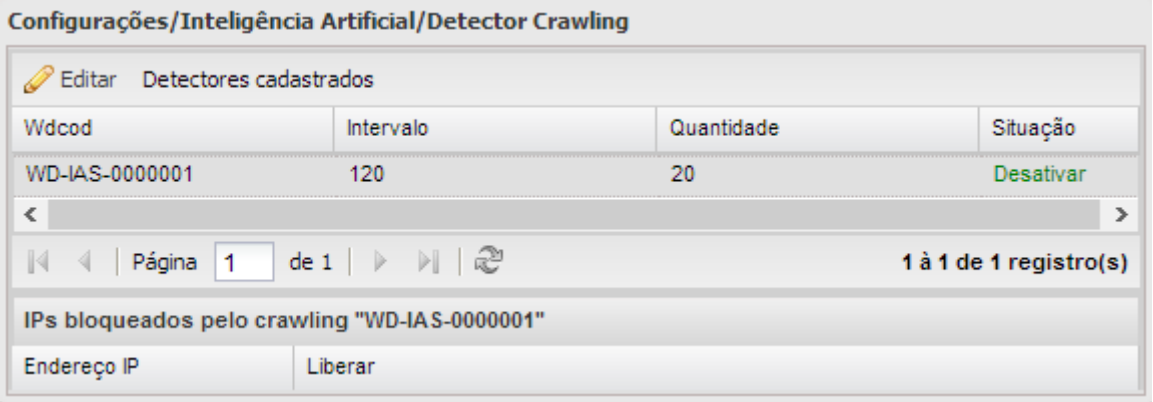


Figura 58 - Detector crawling

4.8. Sistema

No módulo "**Sistema**" o usuário pode definir as configurações de "***Interface, DNS, NTP, visualizar as rotas criadas automaticamente pelo* Aker Web Defender e HTTP Tunning**. A seguir mais detalhes sobre as opções deste módulo:

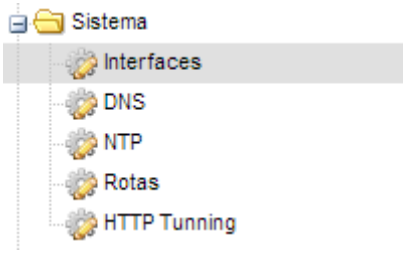


Figura 59 - Sistema

4.9. Interfaces

No módulo "***Interfaces***" permite que o usuário configura as interfaces WAN e LAN, a seguir mais detalhes sobre como configurar interfaces WAN, LAN e inserir IPs adicionais:

Figura 60 - Interfaces

A Interface WAN refere-se ao IP de entrada do **Aker Web Defender**;

Para configura uma interface WAN siga os passos a seguir:

- Digite o número IP da interface e a máscara;

  Ex: IP - 192.168.0.201/ Mask - 255.255.255.0

- Digite o gateway do sistema

  Ex: 192.168.0.1

- Digite a descrição da Interface;

  Ex: WAN

- Selecione o estado da interface;

  Ex: UP

- Clique no botão "**Salvar**".

- A interface LAN refere-se ao IP de saída do **Aker Web Defender**.

  Para configurar o IP saída do **Aker Web Defender** siga os passos a seguir:

- Digite o número IP da interface e a máscara;

  Ex: 31.0.0.1/ Mask - 255.255.255.0
- Digite a descrição da Interface

  Ex: LAN
- Selecione o estado da interface

  Ex: UP
- Clique no botão "***Salvar***".

Para inserir IPs adicionais siga os passos a seguir:

- Digite o número IP da interface;

  Ex: IP - 192.168.0.202
- Selecione o estado da interface;

  Ex: Ativo
- Clique no botão "Salvar".

4.9.1 DNS:

No módulo "***DNS***" o usuário pode configurar o servidor de DNS do **Aker Web Defender.**

Para configurar um servidor de DNS no **Aker Web Defender** siga os passos a seguir:

- Digite o número IP do DNS a ser utilizado;

  Ex: 10.0.0.17
- Clique no botão "***Incluir***".

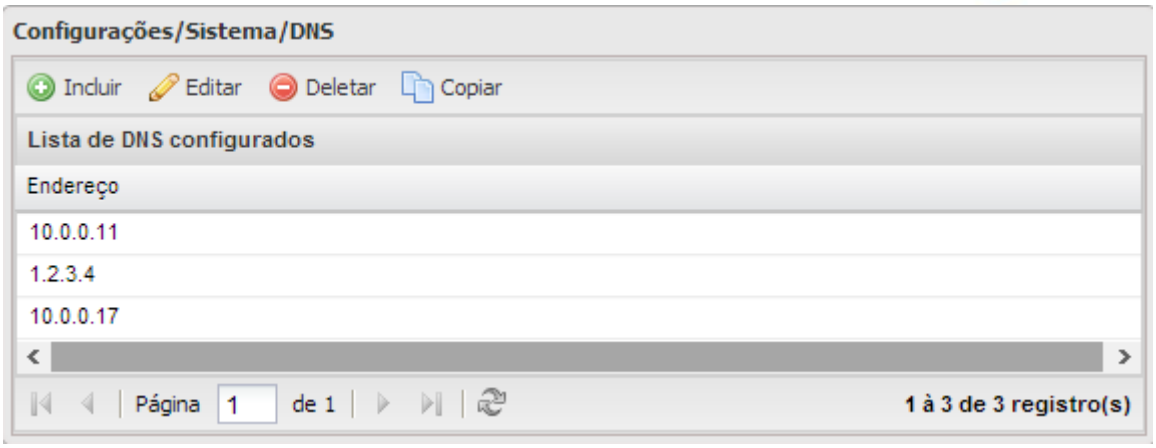


Figura 61 - Aba DNS

4.9.2 NTP:

No módulo "***NTP***" o usuário pode configurar o servidor de NTP do **Aker Web Defender.**

Para configurar um novo servidor NTP no Aker Web Defender siga os passos a seguir:

- Digite o número IP do NTP a ser utilizado ou domínio

Ex: a.ntp.br

- Clique no botão "***Incluir***".

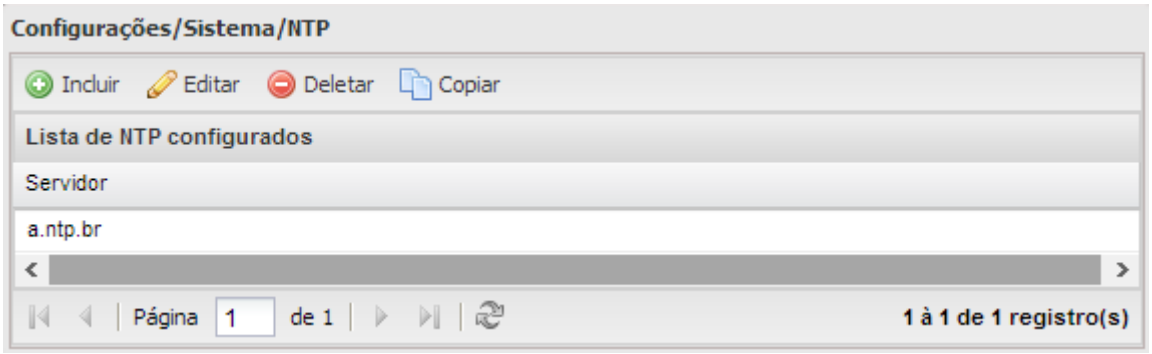


Figura 62 - Aba NTP

4.9.3 ROTAS:

No módulo "***Rotas***" o usuário pode visualizar as rotas do sistema que o Aker Web Defender criou automaticamente quando você cadastrou as interfaces de rede do sistema e os servidores reais.

Rotas de sistema não podem ser editadas, deletadas ou copiadas. Elas são gerenciadas automaticamente pelo Aker Web Defender.

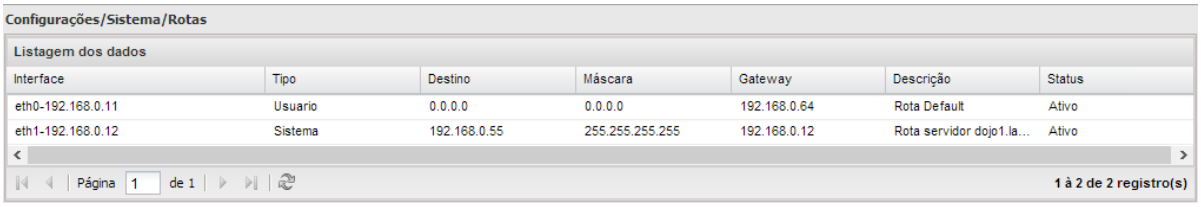


Figura 63 - Aba Rotas

4.9.4 HTTP Tunning

O módulo "***HTTP Tunning***" exibe as configurações do servidor web do Aker Web Defender destinado a receber as conexões dos navegadores. Os parâmetros são ajustados por padrão para oferecer a melhor performance aos usuários.

Caso necessite alterar algum parâmetro deste módulo recomenda-se que entre em contato com o suporte.

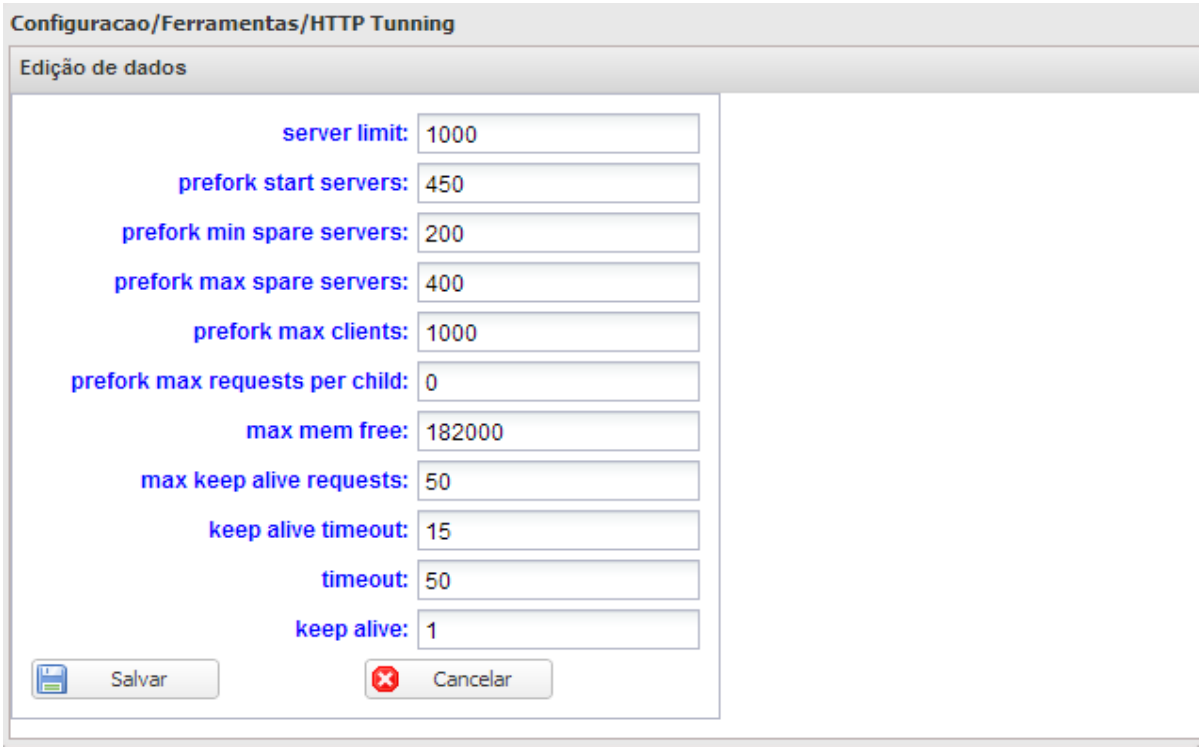


Figura 64 - HTTP Tunning

4.10. Ferramentas

Neste módulo o usuário pode acessar as ferramentas do sistema utilizadas para administrar "***Usuários, Log***", fazer e restaurar "***Backup***".

Figura 65 - Ferramentas

4.10.1 Usuários

Esta aba permite que o Administrador do Aker Web Defender gerencie os usuários do sistema, podendo Incluir, Editar ou Deletar usuários do sistema.

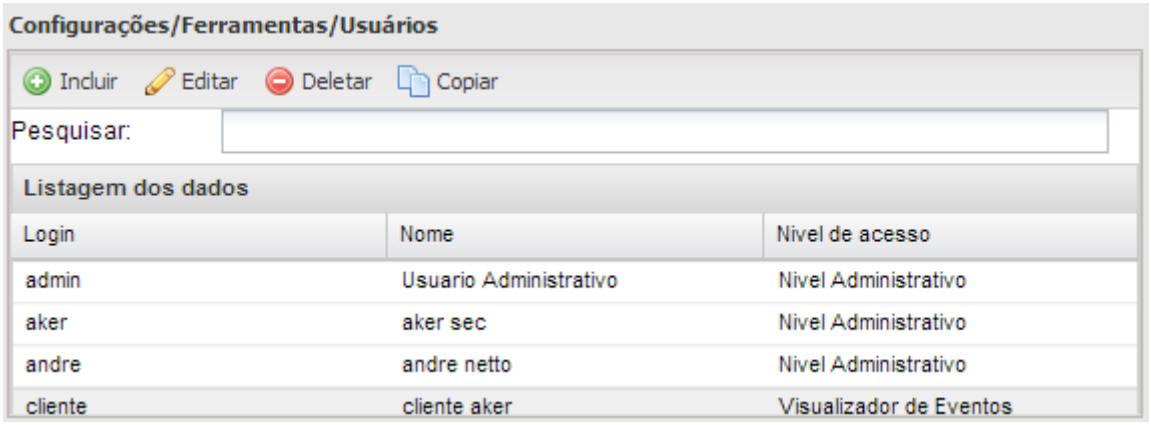


Figura 66 - Aba Usuários

Para incluir um novo usuário siga os passos abaixo:

- Clique no botão "***Incluir***".

Janela de inclusão de usuário

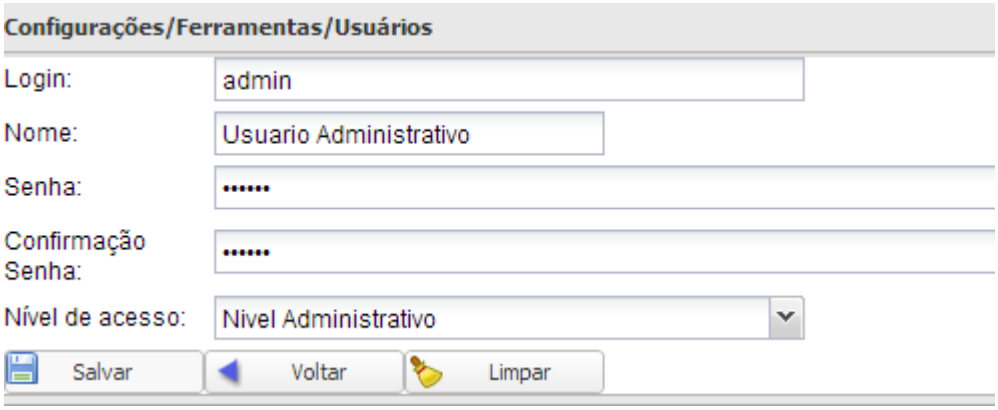


Figura 67 - Janela de inclusão de usuário

Login: Define qual o login que será usado pelo usuário para conectar-se ao Aker Web Defender.

Nome: Define o nome do usuário.

Senha: Define a senha de acesso do usuário.

Confirmação de senha: Insira um a senha novamente para confirmação.

Nível de acesso: Define o nível de acesso do usuário, as opções disponíveis são: **Nível Administrativo e Visualizador de Eventos.**

4.10.2 Log

Nesta aba podemos auditar as entradas de dados no **Aker Web Defender** e quem as realizou.

Nesta aba o usuário terá acesso a todas as ações que foram feitas no Aker Web Defender, especificando a Ação, usuário e horário.

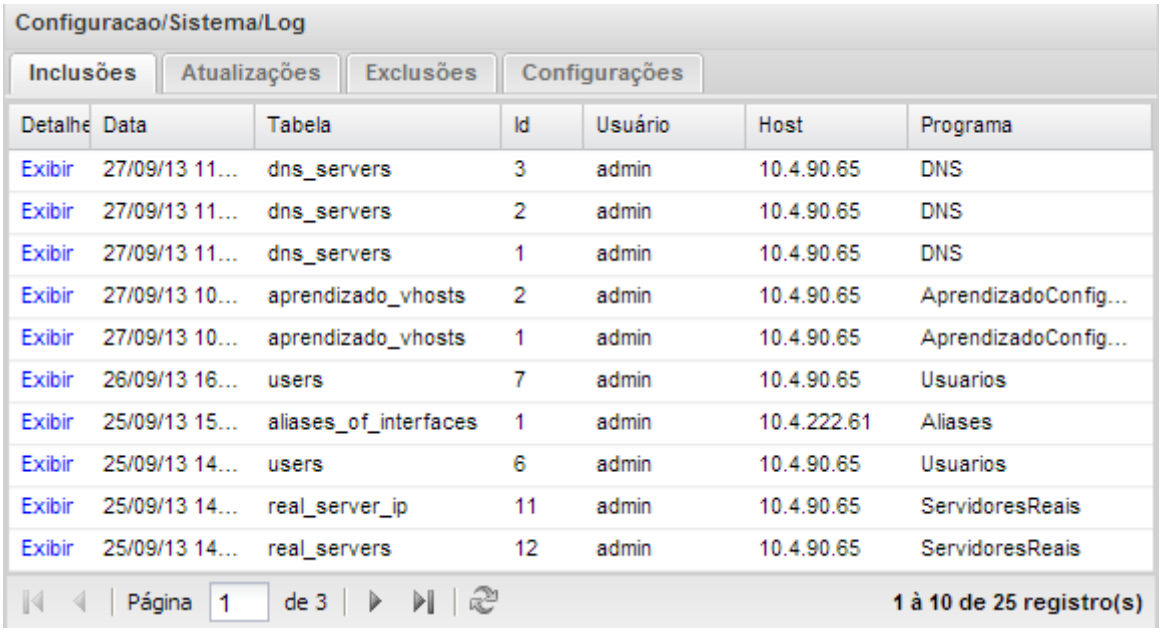

Configuracao/Sistema/Log
Inclusões
Atualizações
Exclusões
Configurações
Detalhe | Data | Tabela | Id | Usuário | Host | Programa
Exibir | 27/09/13 11... | dns_servers | 3 | admin | 10.4.90.65 | DNS
Exibir | 27/09/13 11... | dns_servers | 2 | admin | 10.4.90.65 | DNS
Exibir | 27/09/13 11... | dns_servers | 1 | admin | 10.4.90.65 | DNS
Exibir | 27/09/13 10... | aprendizado_vhosts | 2 | admin | 10.4.90.65 | AprendizadoConfig...
Exibir | 27/09/13 10... | aprendizado_vhosts | 1 | admin | 10.4.90.65 | AprendizadoConfig...
Exibir | 26/09/13 16... | users | 7 | admin | 10.4.90.65 | Usuarios
Exibir | 25/09/13 15... | aliases_of_interfaces | 1 | admin | 10.4.222.61 | Aliases
Exibir | 25/09/13 14... | users | 6 | admin | 10.4.90.65 | Usuarios
Exibir | 25/09/13 14... | real_server_ip | 11 | admin | 10.4.90.65 | ServidoresReais
Exibir | 25/09/13 14... | real_servers | 12 | admin | 10.4.90.65 | ServidoresReais
Página 1 de 3
1 à 10 de 25 registro(s)

Figura 68 - Aba Atualizações

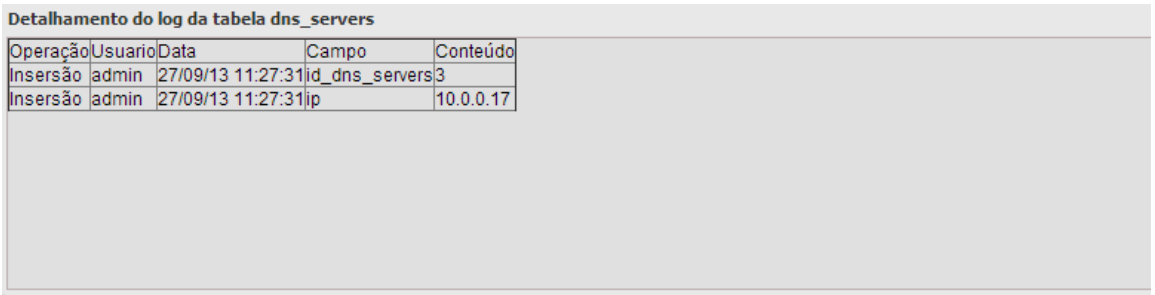

Detalhamento do log da tabela dns_servers
Operação | Usuario | Data | Campo | Conteúdo
Inserção | admin | 27/09/13 11:27:31 | id_dns_servers | 3
Inserção | admin | 27/09/13 11:27:31 | ip | 10.0.0.17

Figura 69 - Detalhamento do log

4.10.3 Backup

Nesta aba é possível que o usuário faça um backup das configurações do **Aker Web Defender**.

É Recomendado que seja feito um backup após cada alteração no sistema.

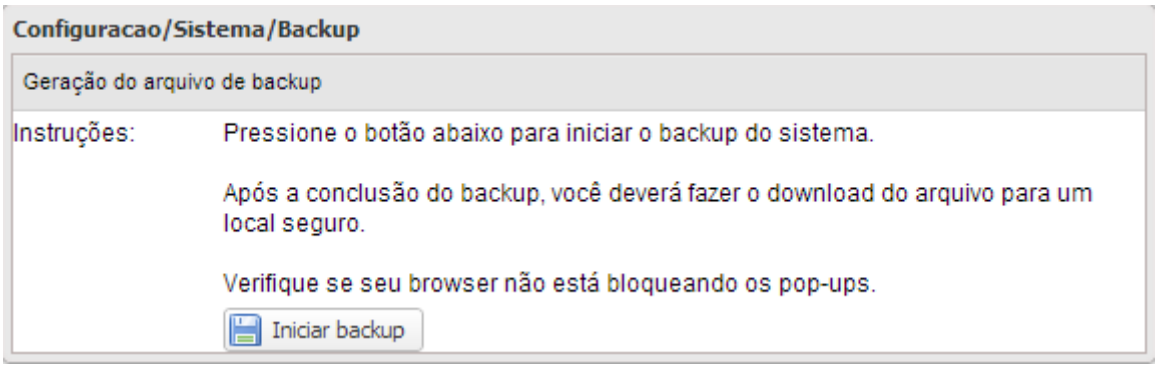

Configuracao/Sistema/Backup
Geração do arquivo de backup
Instruções:
Pressione o botão abaixo para iniciar o backup do sistema.
Após a conclusão do backup, você deverá fazer o download do arquivo para um local seguro.
Verifique se seu browser não está bloqueando os pop-ups.
Iniciar backup

Figura 70 - Aba Backup

4.10.4 Restore

Nesta aba é possível que o usuário faça uma restauração de dados do **Aker Web Defender**, através de um backup criado previamente.

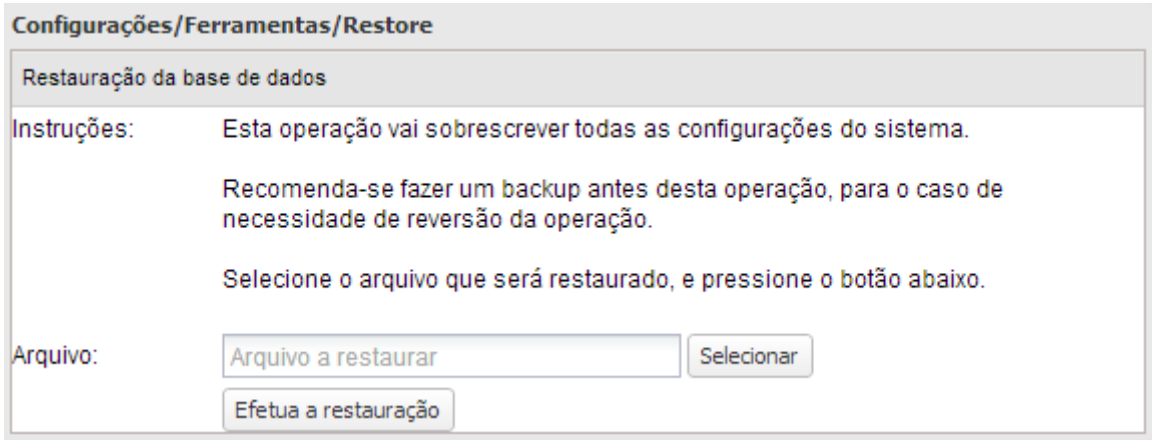

Configurações/Ferramentas/Restore
Restauração da base de dados
Instruções:
Esta operação vai sobrescrever todas as configurações do sistema.
Recomenda-se fazer um backup antes desta operação, para o caso de necessidade de reversão da operação.
Selecione o arquivo que será restaurado, e pressione o botão abaixo.
Arquivo:
Arquivo a restaurar
Selecionar
Efetua a restauração

Figura 71 - Aba Restore

4.11. Configurações

Esta aba permite que o usuário selecione as configurações de navegação da interface gráfica.

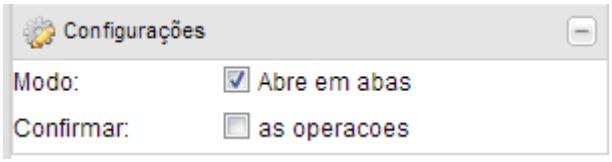


Figura 72 - Configurações

Modo: Define se as janelas de configurações serão abertas em uma janela em abas distintas ou em várias janelas:

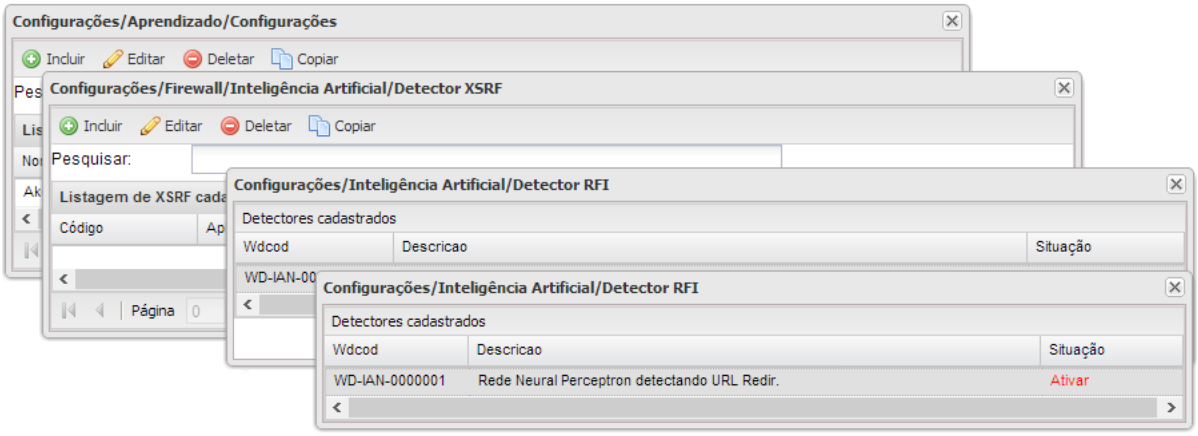


Figura 73 - Modo Janelas

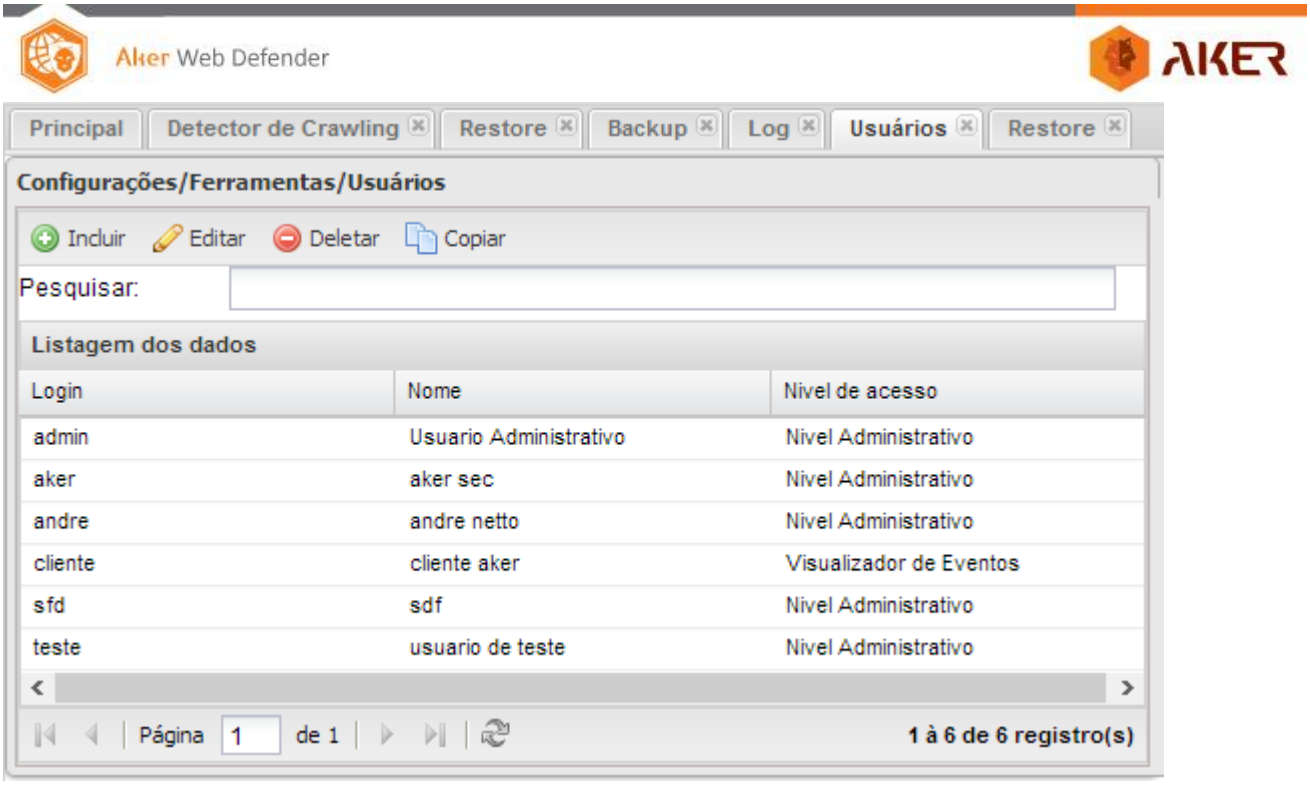


Figura 74 - Modo abas

Confirmar: Ao selecionar esta opção todas as ações feitas necessitaram de uma configuração para que sejam executadas, como na imagem a seguir:

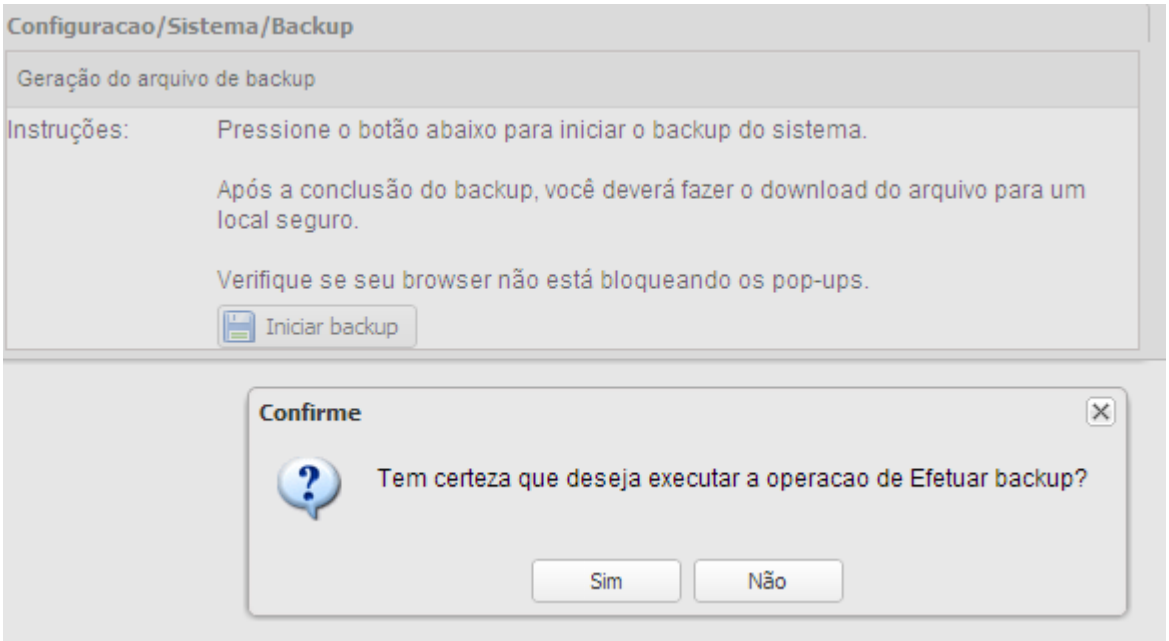

Configuracao/Sistema/Backup
Geração do arquivo de backup
Instruções:
Pressione o botão abaixo para iniciar o backup do sistema.
Após a conclusão do backup, você deverá fazer o download do arquivo para um local seguro.
Verifique se seu browser não está bloqueando os pop-ups.
Iniciar backup
Confirme
Tem certeza que deseja executar a operacao de Efetuar backup?
Sim
Não

Figura 75 - Confirmação para executar ação

F.A.Q

5. F.A.Q

1. **O Aker Web Defender é um *Unified Threat Management (UTM)* com módulos para firewall de aplicação?**

Não, o Aker Web Defender é um appliance especialista e dedicado exclusivamente a fazer análises na camada de aplicação, nos protocolos http e https.

2. **O Aker Web Defender precisa de especialistas para fazer sua instalação?**

Não, o Aker Web Defender foi desenvolvido para atender as empresas sem precisar de professionais sênior para sua instalação e parametrização.

3. **Posso instalar o Aker Web Defender em qualquer distribuição Linux?**

Não, o Aker Web Defender é fornecido em um hardware específico para suportar os mais duros ataques.

4. **Além do Português existe documentação em inglês?**

O Aker Web Defender por ser um produto nacional vem com todas as informações em Português do Brasil, ou seja, tanto o manual do usuário quanto a interface de gerenciamento estão nativamente em idioma português do Brasil, estamos trabalhando em uma versão multi-idiomas e em breve estará disponível no mercado.

5. **É possível que alguns sites possam ser acessados sim passar pelo Firewall de Aplicação?**

Sim, caso haja sites com necessidades específicas da empresa é possível, porém não é recomendável.

6. **O Aker Web Defender trabalha na mesma camada de um IPS?**

Não, o Aker Web Defender é um firewall de aplicação e trabalha diretamente na camada 7 (aplicação) do modelo OSI interceptando todas as requisições e respostas do servidor Web.